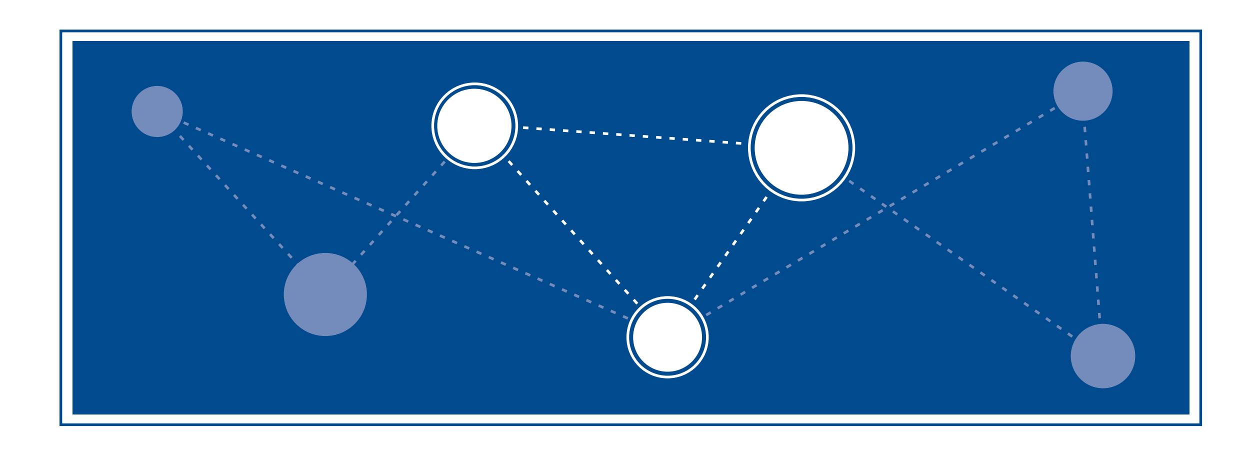


NetScreen Instant Virtual Extranet Platform

Administrationshandbuch



NetScreen Secure Access
NetScreen-SA 1000
NetScreen-SA 3000
NetScreen-SA 5000
NetScreen-SA FIPS

NetScreen Secure Meeting
NetScreen-SM 3000

NetScreen
Instant Virtual Extranet
Plattform

Administrationshandbuch

NetScreen Instant Virtual Extranet-Plattform – Administrationshandbuch, Version 4.1

Verfasser: Carolyn A. Harding und Claudette deGiere

Versionshistorie

17. Juni 2004 – Endgültiger Entwurf

Secure Access Product Group
Juniper Networks, Inc.
940 Stewart Drive
Sunnyvale, CA 94085, USA
Telefon: +1-408-962-8200
Fax: +1-408-962-8201

410A061704

Inhalt

Vorwort

In diesem Handbuch finden Sie die erforderlichen Informationen zum Konfigurieren und Verwalten des NetScreen Instant Virtual Extranet (IVE), unter anderem zu den folgenden Themen:

- Übersicht über die Access Series- und Meeting Series-Produkte und das zugrunde liegende Zugriffsverwaltungssystem
- Übersicht über Basis- und erweiterte Funktionen sowie über Aktualisierungsoptionen
- Anweisungen für die Konfiguration und Verwaltung der IVE-Appliance oder des IVE-Clusters

Zielgruppe

Dieses Handbuch wendet sich an Systemadministratoren, die für die Konfiguration von Access Series- und Meeting Series-Produkten zuständig sind.

NetScreen-SA 1000
NetScreen-SA 3000
NetScreen-SA 5000
NetScreen-SA FIPS
NetScreen-SM 3000

Weiterführende Informationen

Informationen zur Installation können Sie dem Installationshandbuch entnehmen, dass dem Produkt beiliegt. Den neuesten Build des IVE-Betriebssystems mit dem zugehörigen *Administratorhandbuch* im PDF-Format und den Versionshinweisen können Sie auf der Juniper Networks-Supportsite herunterladen.

Teil 1

IVE Series

In diesem Abschnitt werden die NetScreen IVE-Plattform (Instant Virtual Extranet), die Access Series-Produktlinien, die auf dieser Plattform aufbauen, und das Zugriffsverwaltungssystem beschrieben, das von den Access Series-Produkten verwendet wird.

Inhalt

Einführung in das NetScreen Instant Virtual Extranet

Mit dem NetScreen Instant Virtual Extranet können Sie Mitarbeitern, Partnern und Kunden über einen beliebigen Webbrowser überall sicheren und kontrollierten Zugriff auf Datei- und Webserver des Unternehmens, systemeigene Nachrichten- und E-Mail-Clients, gehostete Server und vieles mehr gewähren.

Was ist das NetScreen Instant Virtual Extranet?

Das NetScreen Instant Virtual Extranet oder IVE ist eine gehärtete Netzwerkappliance, die solide Sicherheitsfunktionen bietet. Sie fungiert als Zwischenglied für die Datenströme, die zwischen externen Benutzern und internen Ressourcen übertragen werden. Zu diesen gehören:

- MS Terminal-Server
- MS Exchange-Server
- Lotus Notes-Server
- Internet-E-Mail-Server
- Terminalbasierte Anwendungen (IBM 3270, VT100)
- Dokumente auf Dateiservern
- Webbasierte Unternehmensanwendungen
- Intranetseiten

Mit dem IVE wird es überflüssig, in einer herkömmlichen DMZ Toolkits für Extranets bereitzustellen oder den Mitarbeitern ein VPN (Virtual Private Network) für Remotezugriffe zur Verfügung zu stellen. Die Appliance vermittelt Daten zwischen externen Verbindungen, über die sie sichere Anforderungen erhält, und internen Ressourcen, an die sie Anforderungen für authentifizierte Benutzer sendet.

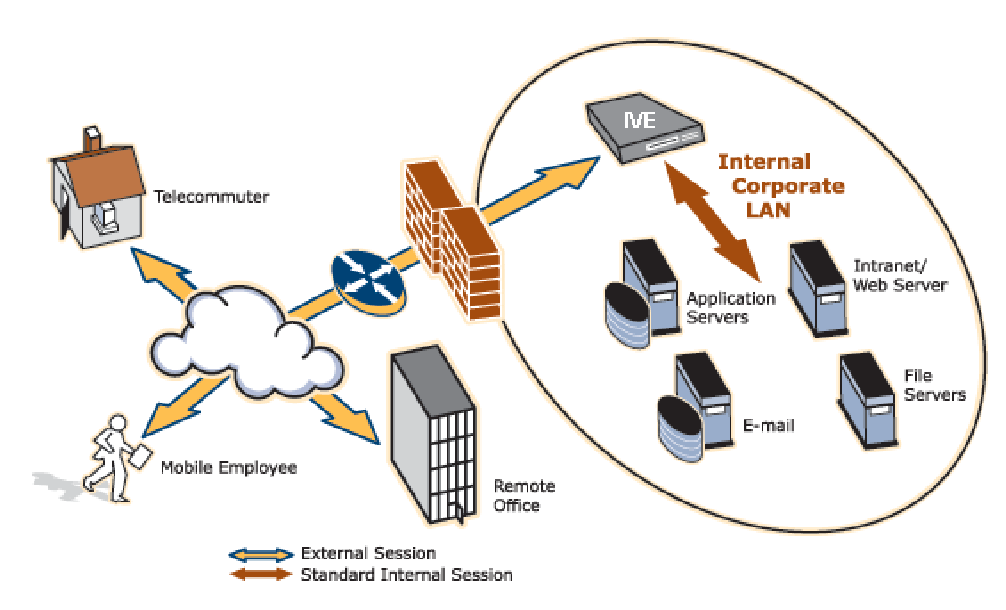


Abbildung 1: **Die IVE-Appliance innerhalb eines LAN**

Wie funktioniert das IVE?

Das IVE arbeitet als sicheres Gateway auf Anwendungsebene, das sämtliche Anforderungen zwischen dem öffentlichen Internet und internen Unternehmensressourcen vermittelt. Auf sämtliche Anforderungen, die das Instant Virtual Extranet erhält, wurde bereits durch den Browser des Endbenutzers eine 128-Bit- oder 168-Bit-SSL/HTTPS-Verschlüsselung angewendet. Unverschlüsselte Anforderungen werden verworfen. Jede Anforderung unterliegt der vom Administrator definierten Zugriffssteuerung, bei der z. B. 2-Faktor-Authentifizierung oder clientseitige digitale Zertifikate eingesetzt werden, bevor sie an die internen Ressourcen weitergeleitet wird. Da das IVE eine stabile Sicherheitsschicht zwischen dem öffentlichen Internet und den internen Ressourcen zur Verfügung stellt, müssen Administratoren nicht fortwährend Sicherheitsrichtlinien verwalten und Sicherheitslücken für zahlreiche verschiedene Anwendungen und Webserver beheben, die in der öffentlichen DMZ bereitgestellt werden.

Das Instant Virtual Extranet vermittelt den Zugriff auf verschiedenste Arten von Anwendungen und Ressourcen mithilfe einfacher Webbrowsertechnologien. Die Benutzer erhalten über eine durch die Appliance gehostete Extranetsitzung einen authentifizierten Zugriff auf autorisierte Ressourcen. Benutzer können von jedem Webbrowser mit Internetanbindung über eine sichere Websitzung auf umfangreiche webbasierte Unternehmensanwendungen, Java-Anwendungen, Dateifreigaben, Terminalhosts und weitere Client/Server-Anwendungen (wie z. B. Microsoft Outlook und Lotus Notes) zugreifen.

Wie wird das IVE konfiguriert?

Die Konfiguration des IVE erfolgt in fünf grundlegenden Schritten über die Webkonsole des Administrators:

1. **Definieren von Benutzer und Administratorrollen**

   Seiten der Webkonsole: **User > Roles** und **Administrators > Delegation**

   Rollensteuerung, auf die Ressourcenbenutzer und Administratoren zugreifen können. Sie können z. B. eine Rolle erstellen, die Benutzern den Zugriff auf Netzwerkverzeichnisse erlaubt und gleichzeitig den Webzugriff verweigert.

   Auf dem IVE sind bereits eine Benutzerrolle („Users") und zwei Administratorenrollen („.Administrators" und „.Read-Only Administrators") vorkonfiguriert.

2. **Definieren von Ressourcenrichtlinien.**

   Seiten der Webkonsole: **Ressourcenrichtlinien**

   Ressourcenrichtlinien dienen zur weiter gehenden Steuerung der Ressourcen, auf die Benutzer und Administratoren zugreifen können. Wenn Sie z. B. den Dateizugriff auf Rollenebene aktiviert haben, können Sie eine Ressourcenrichtlinie erstellen, die den Zugriff auf bestimmte Verzeichnisse im Firmennetzwerk verweigert. Bei der Konfiguration einer Ressourcenrichtlinie müssen Sie die Rollen angeben, für die Ressourcenrichtlinie gelten soll.

   Das IVE ist mit Ressourcenrichtlinien vorkonfiguriert, die allen Benutzern die Web- und Dateisuche erlaubt.

3. **Definieren von Authentifizierungs- und Autorisierungsservern**

   Seiten der Webkonsole: **System > Signing In > Servers**

   Authentifizierungs- und Autorisierungsserver authentifizieren Anmeldeinformationen und ermitteln die Benutzerberechtigungen innerhalb des Systems. Sie können z. B. Benutzer anhand der clientseitigen Zertifikatsattribute über einen Zertifikatsserver authentifizieren und dann einen LDAP-Server verwenden, der Benutzer anhand der Werte autorisiert, die in einer Zertifikatsperrliste (Certificate Revocation List, CRL) aufgeführt sind.

Auf dem IVE sind bereits ein lokaler Authentifizierungsserver für die Benutzerauthentifizierung („System Local") und ein lokaler Authentifizierungsserver für die Administratorauthentifizierung („Administrators") vorkonfiguriert. Sie müssen also zumindest diesen Servern Benutzer hinzufügen, um den Benutzern den Zugriff auf das IVE zu erlauben.

4. **Definieren des Authentifizierungsbereichs**

Seiten der Webkonsole: **Users > Authentication** und **Administrators > Authentication**

Authentifizierungsbereiche enthalten Richtlinien, die die Bedingungen festlegen, die Benutzer und Administratoren für die Anmeldung am IVE erfüllen müssen. Sie können z. B. anhand einer Authentifizierungsrichtlinie angeben, dass Benutzer nur auf das IVE zugreifen können, wenn sie sich von einer bestimmten IP-Adresse aus anmelden oder einen bestimmten Browser verwenden. Beim Konfigurieren eines Authentifizierungsbereichs müssen Sie Regeln erstellen, um Benutzer zu Rollen zuzuordnen und festzulegen, welche(n) Server das IVE für die Authentifizierung und Autorisierung der Bereichsmitglieder verwenden darf.

Auf dem IVE ist bereits ein Bereich („Users") vorkonfiguriert, der alle über den Server „System Local" authentifizierten Benutzer der Rolle „Users" zuordnet. Außerdem ist auf dem IVE bereits ein Bereich („Admin Users") vorkonfiguriert, der alle über den Server „Administrators" authentifizierten Benutzer der Rolle „.Administrators" zuordnet.

5. **Definieren von Anmelderichtlinien**

Seite der Webkonsole: **System > Signing In > Sign-In Policies**

Anmelderichtlinien definieren die URLs, die Benutzer und Administratoren für die Anmeldung am IVE verwenden können. Sie können z. B. Anmelderichtlinien verwenden, um einen Anmelde-URL für die Abteilung „Vertrieb" und einen anderen für die Abteilung „Versand" zu erstellen. Bei der Konfiguration einer Anmelderichtlinie müssen Sie diese mindestens einem Bereich zuordnen. Es können sich dann nur Mitglieder des angegebenen Bereichs bzw. der angegebenen Bereiche anhand des URLs, der in der Richtlinie angegeben wurde, am IVE anmelden.

Auf dem IVE ist bereits eine Anmelderichtlinie vorkonfiguriert, die den Benutzern des Bereichs „Admin Users" erlaubt, sich anhand des URLs „*/admin" anzumelden, sowie eine weitere, die den Mitgliedern des Bereichs „Users" gestattet, sich anhand des URLs „*/" anzumelden.

Access Series – Übersicht

Die Juniper Networks NetScreen Secure Access-Produktfamilie bietet ein hohes Maß an Skalierbarkeit für Unternehmen, hohe Verfügbarkeit sowie Sicherheitsfunktionen, um den sicheren Zugriff auf Netzwerkressourcen zu erweitern. Das Access Series Instant Virtual Extranet (IVE) kann innerhalb weniger Stunden konfiguriert werden, um Benutzern sicheren Zugriff auf die folgenden Elemente zu ermöglichen:

- Interne Unternehmenswebsites und webbasierte Anwendungen, darunter clientseitige Java-Applets, unter Verwendung von Desktopcomputern, Laptopcomputern und drahtlosen Pocket PC-Geräten (Standard)
- Interne Dateiserver (NFS und CIFS) des Unternehmens sowie Funktionen zur Dateiübertragung zu und von beliebigen Verzeichnissen (Standard)
- Systemeigene Nachrichtenclients wie Microsoft Outlook und IBM/Lotus Notes von jedem PC aus (Aktualisierungsoption für Secure Email Client)
- Auf Standards basierende E-Mail-Clients wie Microsoft Outlook Express, Netscape Communicator und Eudora von Qualcomm von jedem PC aus (Aktualisierungsoption für Secure Application Manager)
- Client-/Serveranwendungen wie Citrix ICA Client, pcAnywhere und MS-Terminaldienste von jedem PC aus (Aktualisierungsoption für Secure Application Manager)
- Gehostete Server über Telnet und SSH von jedem PC aus (Aktualisierungsoption für sicheren Terminalzugriff)
- Funktionen für die sichere Zusammenarbeit, einschließlich der Planung von Konferenzen, Remote-Konferenzvorführungen, Remotesteuerung des Desktops des Vorführenden sowie Textchats (Aktualisierungsoption Secure Meeting)

Ihre Mitarbeiter, Partner und Kunden benötigen lediglich einen Standardwebbrowser für den PC (Internet Explorer/Netscape/AOL/Pocket IE) und eine Internetverbindung für den Zugriff auf die intuitive Startseite des Access Series IVE. Auf dieser Seite wird das Fenster bereitgestellt, über das die Benutzer sicher Web- oder Dateiserver durchsuchen, HTML-fähige Unternehmensanwendungen verwenden, den Client-/Serveranwendungsproxy starten oder eine Terminalsitzung beginnen können[1].

1. Die verfügbaren Funktionen hängen von dem erworbenen Produkt der NetScreen Access Series und den erworbenen Aktualisierungsoptionen ab.

Die Installation, Konfiguration und Verwaltung des IVE sind unkompliziert. Bei dem IVE handelt es sich um eine Netzwerkappliance, die innerhalb weniger Minuten im Rack montiert werden kann. Sobald eine Verbindung mit Ihrem Netzwerk besteht, müssen Sie an der seriellen Konsole nur noch einige System- und Netzwerkeinstellungen eingeben, um auf die Webkonsole zuzugreifen. Die Webkonsole ist die Webschnittstelle, über die Sie das IVE nach den Anforderungen Ihres Unternehmens konfigurieren und verwalten können. Die folgenden Features ermöglichen eine problemlose Bereitstellung und effiziente Wartung des Systems:

- Einfache Serverintegration – Das IVE lässt sich in vorhandene Authentifizierungsserver (LDAP, RADIUS, NIS, Windows NT-Domäne, Active Directory und RSA-ACE/Server) des Unternehmens integrieren. Sie müssen keine Änderungen an den internen Webservern, Dateiservern oder Netzwerken vornehmen.
- Zertifikatauthentifizierung – Schützt Anwendungen ohne Änderungen an den internen Ressourcen. Sie wählen lediglich die digitalen Zertifikate als Teil des Authentifizierungsschemas für das Access Series IVE aus.
- Hohe Verfügbarkeit und Redundanz – Keine Ausfallzeit für die Benutzer im seltenen Fall eines Systemausfalls und „Stateful Peering", durch das die Benutzereinstellungen, die Systemeinstellungen und die Sitzungsdaten der Benutzer synchronisiert werden (in einer Cluster-Umgebung).
- Einfache Firewallrichtlinien – Von außen ist nur ein SSL-Zugriff auf die IVE-Appliance erforderlich.
- Ressourcenzugriffskontrolle auf der Ebene der Dateien und URLs, die das IVE 4.0 Zugriffsverwaltungssystem verwenden (Authentifizierungsbereiche, Benutzerrollen und Ressourcenrichtlinien).
- Zentralisierte Protokollierung auf Anwendungsebene, durch die Administrator- und Benutzeraktionen, Verbindungs-, Datei- und Webanforderungen sowie Systemfehler verfolgt werden.
- Systemsoftwareaktualisierungen über das Internet.
- SNMP- und DMZ-Unterstützung.

Access Series FIPS – Übersicht

FIPS oder ***Federal Information Processing Standards (Bundesstandards für Informationsverarbeitung)*** sind Bestimmungen des NIST (National Institute of Standards and Technology) für die Behandlung von Schlüsseln und verschlüsselten Daten. NetScreen Access Series FIPS ist ein Standard-A5000- oder A3000-NetScreen Instant Virtual Extranet, das mit einem Kryptographiemodul mit FIPS-Zertifikat ausgerüstet ist. Das auf einem Access Series FIPS-System installierte manipulationssichere Hardwaresicherheitsmodul erfüllt die Sicherheitsanforderungen des FIPS 140-2-Zertifikats der Ebene 3. Das Modul verwaltet private Kryptographieschlüssel und führt SSL-Handshakes durch. Dabei stellt es die Kompatibilität mit FIPS sicher und delegiert rechenintensive PKI-Aufgaben (Public Key Infrastructure) von der Appliance an das dedizierte Modul.

Administratoren für Access Series FIPS-Geräte müssen im Prinzip die gleichen Konfigurationsaufgaben wie andere Administratoren durchführen, die nicht dem Standard von FIPS Access Series entsprechen. Nur bei der Initialisierung, Clusterbildung und Zertifikatserzeugung sind kleinere Konfigurationsänderungen erforderlich. Für die wenigen Fälle, in denen die Verwaltungsaufgaben abweichen, enthält dieses Handbuch die entsprechenden Anweisungen für Access Series- und Access Series FIPS-Administratoren. Für Endbenutzer ist Access Series FIPS dasselbe wie ein Access Series-Standardsystem.

Wie funktioniert NetScreen Access Series FIPS?

Bei der Erstinstallation eines Access Series FIPS-Systems werden Sie über die serielle Konsole des IVE durch die Schritte zum Einrichten einer Security World geführt. Eine ***Security World*** ist ein von Access Series FIPS verwendetes Schlüsselmanagementsystem, das sich aus den folgenden Elementen zusammensetzt:

- **Kryptographiemodul** – Das Kryptographiemodul (auch als Hardwaresicherheitsmodul oder HSM bezeichnet) von Access Series FIPS enthält Hardware und Firmware, die direkt in der Appliance installiert wird. Eine Security World kann aus einem einzelnen Kryptographiemodul (Standardumgebung) oder verschiedenen Modulen (Clusterumgebung) bestehen. Eine einzelne Access Series FIPS-Appliance ist aber immer mit einem Kryptographiemodul ausgestattet.

- **Security World-Schlüssel** – Ein Security World-Schlüssel ist ein eindeutig verschlüsselter Triple DES-Schlüssel, der die Sicherheit aller anderen Anwendungsschlüssel in einer Security World gewährleistet. Die Federal Information Processing Standards (FIPS) schreiben vor, dass dieser Schlüssel nicht in eine Security World importiert werden kann, sondern direkt in einem Kryptographiemodul erzeugt werden muss. In einer Clusterumgebung verwenden alle Module in der Security World denselben Security World-Schlüssel. (Weitere Informationen finden Sie unter „Bereitstellen eines Clusters in einer Access Series FIPS-Umgebung" auf Seite 85.)
- **Smartcards** – Eine Smartcard ist ein transportabler Schlüssel, der wie eine Kreditkarte aussieht. Benutzer können sich mithilfe einer Smartcard authentifizieren, um auf verschiedene Daten und Prozesse, die vom Kryptographiehardwaremodul gesteuert werden, zuzugreifen. Beim Initialisierungsvorgang muss der mit dem Kryptographiemodul gelieferte Smartcardleser angeschlossen und dann eine Smartcard in den Leser eingelegt werden. Während des Initialisierungsvorgangs wird die Smartcard in eine ***Administratorkarte*** umgewandelt, die dem Karteninhaber den Zugriff auf die Security World gestattet. (Weitere Informationen finden Sie unter „Erstellen weiterer Administratorkarten (nur Access Series FIPS)" auf Seite 574.)
- **Verschlüsselte Daten** – Verschlüsselte Hostdaten in einer Access Series FIPS-Umgebung enthalten Schlüssel und andere Daten, die für die sichere Freigabe von Informationen erforderlich sind.

Diese Elemente sind aufeinander abgestimmt, um eine umfassende Security World zu erstellen. Beim Starten der Appliance wird die Gültigkeit der Security World überprüft und ermittelt, ob sich das Kryptographiemodul im Operationsmodus befindet, bevor der normale Betrieb aufgenommen wird.

Sie können das Kryptographiemodul mithilfe eines am Modul befindlichen Hardwareschalters in den Operationsmodus schalten. Es gibt folgende Schaltereinstellungen:

- **I** – Initialisierungsmodus. Verwenden Sie diese Einstellung, um das Kryptographiemodul mit einer neuen Security World zu initialisieren oder um ein Modul zu einer bestehenden Security World in einem IVE-Cluster hinzuzufügen. Beachten Sie, dass der Prozess abgeschlossen werden muss, sobald der Schalter auf I gesetzt und mit der Initialisierung begonnen wurde. Andernfalls wird die Security World nur teilweise initialisiert und ist somit nicht verwendbar.

- **O** – Operationsmodus. Mit dieser Einstellung können Sie das Kryptographiemodul nach der Initialisierung in den Operationsmodus versetzen. Beachten Sie, dass Sie den Schalter vor dem Einschalten des Moduls auf **O** setzen müssen, damit das Gerät mit der Routineverarbeitung beginnt. Andernfalls müssen Sie an der seriellen Konsole angeben, ob Sie sich mit der vorhandenen Security World verbinden oder eine neue initialisieren möchten.
- **M** – Wartungsmodus (Maintenance). In künftigen Versionen kann die Firmware auf dem Kryptographiemodul mit dieser Einstellung aktualisiert werden. (Bisher nicht unterstützt.)

Weitere Informationen zum Initialisieren des Moduls und Erstellen einer neuen Security World finden Sie im beiliegenden Leitfaden für die ersten Schritte.

Erstellen von Administratorkarten

Im Lieferumfang des Access Series FIPS sind sechs Smartcards enthalten. Eine ***Smartcard*** ist ein transportabler Schlüssel, der für den Zugriff auf zentrale Daten und Prozesse erforderlich ist, die vom Kryptographiemodul gesteuert werden. Bei der Initialisierung des Kryptographiemoduls über die serielle Konsole werden Sie von Access Series FIPS zunächst dazu aufgefordert, eine Smartcard zu verwenden. Während dieses Vorgangs erstellt Access Series FIPS eine Security World und wandelt die Smartcard in eine ***Administratorkarte*** um, die dem Karteninhaber exklusiven Zugriff auf die Security World gewährt.

Die Administratorkarte wird nur zum Initialisieren des Moduls benötigt. Für den normalen IVE-Betrieb nach der Initialisierung ist sie nicht erforderlich. Die Administratorkarte ist zum Durchführen der folgenden Aktionen erforderlich:

- Hinzufügen eines weiteren Access Series FIPS-Geräts zu einem Cluster (Seite 229)
- Neuinitialisieren eines Moduls mit einer neuen oder einer anderen Security World (Seite 576)
- Erstellen weiterer Administratorkarten (Seite 574)

Als Faustregel gilt, dass für jede Access Series FIPS-Operation, die in der seriellen IVE-Konsole ausgeführt werden muss, eine Administratorkarte erforderlich ist.

Hinweis: Bei jeder Änderung der Security World müssen Sie bestimmen, wie die vorhandenen Administratorkarten verwendet werden. Folgende Optionen stehen zur Verfügung:
– Sie richten die vorhandenen Administratorkarten für die neue Security World neu ein.
– Sie verwenden Administratorkarten, die für die neue Security World vorinitialisiert sind und lassen die vorhandenen Administratorkarten unverändert. Beachten Sie aber, dass Sie bei dieser Option die alten, nicht geänderten Karten nicht zum Zugriff auf die neue Security World verwendet werden können.

Da Administratorkarten für Access Series FIPS-Operationen und die Sicherheit innerhalb Ihrer Security World von entscheidender Bedeutung sind, werden folgende Sicherheitsmaßnahmen dringend empfohlen:

- **Erstellen mehrerer Administratorkarten**

  Sie können Administratorkarten nur ersetzen, wenn Sie eine andere gültige Karte besitzen und das Kennwort für den Kartensatz kennen. Das Kryptographiemodul speichert keine Wiederherstellungsdaten für Administratorkarten. Daher wird dringend empfohlen, dass Sie mindestens eine Administratorkarte für die Durchführung administrativer Standardaufgaben und eine weitere als Ersatz erstellen. Andernfalls laufen Sie Gefahr, Ihre einzige Administratorkarte und damit den Zugriff auf Ihre Security World und alle darin gespeicherten Daten zu verlieren.

- **Aufbewahren einer Ersatzadministratorkarte an einem sicheren Ort**

  Bewahren Sie Ihre Ersatzadministratorkarten an einem sicheren Ort und nicht zusammen mit der Karte auf, die Sie für die täglichen Verwaltungsaufgaben verwenden, damit nicht alle Administratorkarten auf einmal verloren gehen können (z. B. durch Feuer oder Diebstahl).

- **Überschreiben aller verbleibenden Administratorkarte bei Verlust einer Karte**

  Bei Verlust oder Beschädigung einer Administratorkarte sollten Sie umgehend eine neue Security World erstellen und alle verbleibenden Karten der alten Security World überschreiben. Andernfalls kann ein Angreifer mit einer alten Administratorkarte u. U. auf die alten Hostdaten auf einem Sicherungsband oder einem anderen Host zugreifen. Mit den alten Hostdaten und einer Karte ist der Angreifer dann vielleicht in der Lage, neue Schlüssel zu erstellen.

- **Schützen des Kennworts einer Administratorkarte**

  Für maximale Sicherheit sollten Sie Ihr Kennwort nie aufschreiben oder nicht vertrauenswürdigen Benutzern mitteilen. Verwenden Sie auch keine Kennwörter, die einfach zu erraten sind. Die Sicherheit Ihres Kennwortes erhöht die Sicherheit der von Ihnen durchgeführten Operationen.

- **Verwenden von Administratorkarten aus ausschließlich bekannten und vertrauenswürdigen Quellen**

  Verwenden Sie nur Smartcards aus vertrauenswürdigen Quellen, legen Sie Smartcards nie in nicht vertrauenswürdige Smartcardleser ein, und legen Sie keine nicht vertrauenswürdigen Smartcards in Ihren Smartcardleser ein.

Secure Meeting – Übersicht

Mit Secure Meeting können IVE-Benutzer Onlinekonferenzen sicher planen und durchführen, an denen sowohl IVE-Benutzer als auch Nicht-IVE-Benutzer teilnehmen können. Während einer Konferenz kann ein Benutzer seinen Desktop und seine Anwendungen über eine sichere Verbindung freigeben, sodass seine elektronischen Daten umgehend auch auf den Bildschirmen der anderen Teilnehmer vorliegen. Mit der Desktop-Remotesteuerung und über Textchats in einem separaten, von der Vorführung unabhängigen Fenster können die Konferenzteilnehmer auch sicher online zusammenarbeiten. Juniper Networks bietet Secure Meeting auf zwei verschiedenen Appliances an:

- **Meeting Series-Appliance** – Die Meeting Series-Appliance ist ein dedizierter Konferenzserver für Umgebungen, in denen häufig Konferenzen abgehalten werden.
- **Access Series-Appliance mit Secure Meeting-Aktualisierung** – Die Secure Meeting-Aktualisierung ist auf Benutzer der Access Series zugeschnitten, die nur in begrenztem Umfang Konferenzen durchführen. Bei dieser Option vermittelt der Server, auf dem die Konferenzen durchgeführt werden, auch Anforderungen zwischen dem öffentlichen Internet und den internen Unternehmensressourcen.

Der Konfigurationsprozess für Meeting Series- und Access Series-Administratoren ist fast identisch, da beide Appliances auf der IVE-Plattform aufbauen. Für die wenigen Fälle, in denen die Verwaltungsaufgaben abweichen, enthält dieses Handbuch die entsprechenden Anweisungen für Access Series- und Meeting Series-Administratoren.

Eine Übersicht über die Funktionen und Systemanforderungen finden Sie unter:

Konfigurationsanweisungen finden Sie unter:

Anweisungen für die Überwachung und Fehlerbehebung finden Sie unter:

Hinweis: Die hier aufgeführten Anweisungen ergänzen die Standard-Konfigurationsanweisungen für das IVE, die in diesem Handbuch aufgeführt sind.

Secure Meeting-Verwendung

Secure Meeting beinhaltet folgende Funktionen:

Konferenzplanung

Jede Secure Meeting-Onlinekonferenz muss durch einen IVE-Benutzer geplant werden. Über die sichere Gatewayschnittstelle stellt der ***Ersteller der Konferenz*** die Konferenzdetails bereit, einschließlich Konferenzname, Beschreibung, Startzeit, Startdatum, Wiederholungsmuster, Dauer, Kennwort, Gästeliste und E-Mail-Adressen der Gäste.

Beim Zusammenstellen einer Gästeliste muss der Ersteller der Konferenz die Gäste einer der zwei folgenden Kategorien zuordnen:

- **IVE-Gast** – Ein IVE-Gast (auch als netzinterner Gast bezeichnet) ist ein IVE-Benutzer, der sich bei derselben IVE-Appliance bzw. bei demselben Cluster wie der Ersteller der Konferenz anmeldet.
- **Nicht-IVE-Gast** – Ein Nicht-IVE-Gast (auch als netzexterner Gast bezeichnet) ist ein Nicht-IVE-Benutzer oder ein IVE-Benutzer, der sich bei einer anderen IVE-Appliance bzw. bei einem anderen Cluster als der Konferenzersteller anmeldet.[1]

1. Secure Meeting gewährleistet zwar, dass Gäste ohne IVE bei der Anmeldung ihren Namen eingeben müssen, die Namen werden aber nicht authentifiziert. Zur Authentifizierung von Personen ohne IVE verwendet Secure Meeting nur die Konferenz-IDs und Kennwörter.

Wenn der Konferenzersteller die Konferenz speichert, wird diese von Secure Meeting auf der Seite **Meetings** für die der Konferenz zugeordneten IVE-Gäste angezeigt.[1] Wenn Sie einen SMTP-Mailserver (Simple Mail Transfer Protocol) aktivieren, sendet Secure Meeting außerdem eine Benachrichtigungs-E-Mail an alle Gäste mit einer bekannten E-Mail-Adresse. Secure Meeting ruft die E-Mail-Adressen aus zwei Quellen ab:

- **Seite „Preferences"** – Ein IVE-Benutzer kann seine E-Mail-Adresse auf der Seite **Preferences** auf der IVE-Startseite angeben. In diesem Fall wird von Secure Meeting automatisch diese Adresse verwendet, wenn der Teilnehmer zu einer Konferenz eingeladen wird.
- **Seite „Create Meeting"** – Der Konferenzersteller kann die E-Mail-Adressen von Konferenzteilnehmern manuell eingeben (oder überschreiben), wenn er eine Konferenz plant oder aktualisiert.

Die E-Mail-Nachricht enthält Konferenzdetails und eine Verknüpfung, über die der Gast der Konferenz beitreten kann, sowie eine weitere Verknüpfung, über die der Gast überprüfen kann, ob sein System mit Secure Meeting kompatibel ist. Teilnehmer können einer Konferenz bis 15 Minuten vor ihrem Start beitreten. (Weitere Informationen finden Sie unter „Von Secure Meeting unterstützte Umgebungen" auf Seite 21.)

Erstellen von Sofortkonferenzen

Durch Erstellung einer ***Sofortkonferenz*** kann die Konferenzplanung erheblich abgekürzt werden. Mit der Funktion für Sofortkonferenzen können IVE-Benutzer in zwei einfachen Schritten eine Konferenz erstellen und dieser beitreten. Zunächst müssen die Benutzer auf **Instant Meeting** klicken. Anschließend führt Secure Meeting automatisch folgende Aktionen aus:

- Erstellung einer Konferenz mit einem eindeutigen Namen und Kennwort
- Planung der Konferenz für sofortigen Beginn
- Festlegen der Dauer auf 60 Minuten
- Hinzufügen des Konferenzerstellers als einzigen Gast
- Aufrufen der Seite **Join Meeting** auf dem Desktop des Konferenz-erstellers

Anschließend kann der Konferenzersteller beginnen, indem er einfach auf **Start Meeting** klickt.

1. Wenn Sie Secure Meeting auf Rollenebene deaktivieren, kann die Seite „Meetings" von Benutzern, die für diese Rolle angemeldet sind, nicht angezeigt werden, selbst wenn sie zu einer Konferenz eingeladen sind.

Sofortkonferenzen werden häufig für Support-Konferenzen verwendet. Angenommen, ein Kunde benötigt die Hilfe eines IVE-Benutzers beim Lösen eines Problems mit einer Anwendung. Mit Secure Meeting kann der IVE-Benutzer in kurzer Zeit eine Sofortkonferenz erstellen und den Kunden als Vorführenden bestimmen. Der Kunde kann die betreffende Anwendung dann öffnen und freigeben. Wenn der Kunde sein Problem nachspielt, kann der IVE-Benutzer im Secure Meeting-Betrachterfenster einfach die Vorgehensweise des Kunden verfolgen. Anschließend kann der IVE-Benutzer das Problem beheben oder über die Steuerungsfunktion die Schritte zur Fehlerbehebung demonstrieren. Der Kunde muss dem IVE-Benutzer lediglich die Steuerung überlassen, damit dieser die freigegebene Anwendung mit seiner eigenen Maus und Tastatur bedienen kann.

Hinweis: Da der Konferenzersteller der einzige Gast der Sofortkonferenz ist, kann er nicht auf E-Mail-Benachrichtigungen zurückgreifen, um andere Konferenzteilnehmer über Details zu informieren. Stattdessen muss er anderen Teilnehmern die für die Konferenzteilnahme erforderlichen Informationen zusenden, z. B. URL, ID und Kennwort (das auf der Seite **Join Meeting** bereitgestellt wird), oder er muss wieder zur Seite **Meeting Details** nach dem Erstellen der Konferenz zurückwechseln und Gäste manuell hinzufügen. Da der Konferenzersteller auch der einzige IVE-Teilnehmer ist, kann er als Einziger die Konferenz leiten.

Beitreten zu Konferenzen

Für die Teilnahme an einer Konferenz müssen Secure Meeting-Teilnehmer über einen der folgenden Schritte zur Konferenzsite auf dem Secure Meeting-Server (IVE)[1] wechseln:

- Über die Verknüpfung auf der Seite **Meetings** (nur IVE-Teilnehmer)
- Über die Verknüpfung in der Benachrichtigungs-E-Mail
- Durch Eingabe des Konferenz-URLs in einem Webbrowser

Der Konferenzersteller kann den URL einer Konferenz auf der Seite **Join Meeting** abrufen. Auch jeder Konferenzteilnehmer kann den Konferenz-URL ermitteln, indem er unter folgendem URL die entsprechenden Werte eingibt:

```
https://<IhrIVE>/meeting/<KonferenzID>
```

1. Secure Meeting hält Onlinekonferenzen auf dem IVE ab, an denen sowohl IVE-Benutzer als auch Nicht-IVE-Benutzer teilnehmen können. Allerdings haben Konferenzteilnehmer ohne IVE nur Zugriff auf die Konferenz, zu der sie eingeladen wurden, nicht auf die anderen Ressourcen im IVE.

Dabei gilt:

- `<IhrIVE>` ist der Name und die Domäne des IVE, auf dem die Konferenz stattfindet, z. B. `iveserver.firmenname.com`. Dieser Name wird von Secure Meeting aus dem Feld **Hostname** auf der Registerkarte **System > Network > Overview** übernommen, sofern er dort angegeben wurde. Andernfalls übernimmt Secure Meeting den IVE-Namen aus dem Browser des Konferenzerstellers.
- `meeting` ist eine Literalzeichenfolge. (Diese Zeichenfolge wird nicht verändert.) Beachten Sie, dass `meeting` mit einem klein geschriebenem „m" beginnen muss.
- `<KonferenzID>` ist die eindeutige Kennnummer aus 8 Ziffern, die von Secure Meeting für diese Konferenz generiert wird. Wenn der Benutzer die ID nicht in den URL einfügt, wird er von Secure Meeting bei der Konferenzanmeldung zur Eingabe des URLs aufgefordert.

Beispiel:

```
https://connect.acmegizmo.com/Meeting/86329712
```

Konferenzteilnahme

Wenn ein Gast der Konferenz beitritt, lädt Secure Meeting einen Windows-Client oder ein Java-Applet[1] auf das System des Gastes herunter. Die Clientkomponente enthält einen Konferenz-Betrachter, Präsentationstools und eine Anwendung zur Übermittlung von Textnachrichten. Nachdem Secure Meeting den Windows-Client oder das Java-Applet auf dem Desktop des Benutzers gestartet hat, wird der Benutzer zum ***Konferenzteilnehmer*** und kann sich an der Konferenz beteiligen. Sobald ein Teilnehmer einer Konferenz beigetreten ist, kann er im Fenster **Secure Meeting Chat** Textnachrichten an andere Teilnehmer senden.

---

1. Secure Meeting lädt ein Java-Applet für Benutzer anderer Betriebssysteme als Windows herunter. Beachten Sie, dass Benutzern die Meldung „Secure Meeting-Client wird installiert, bitte warten Sie..." für unbestimmte Zeit angezeigt wird, wenn von Secure Meeting versucht wird, über die Sun JVM ein Java-Applet auszuführen, und sich eine Datei „proxy.pac" auf dem lokalen System des Benutzers befindet. Dieses Problem wird behoben, indem der Benutzer über Systemsteuerung > Java Plug-in auf die Registerkarte Proxies wechselt, das Kontrollkästchen Browser-Einstellungen verwenden deaktiviert und im Feld für den URL der automatischen Proxy-Konfiguration den URL der PAC-Datei eingibt (z. B. http://10.10.10.10/proxy.pac)

Konferenzdurchführung

Der ***Konferenzleiter*** ist für das Starten der Konferenz verantwortlich und muss einen Vorführenden benennen. Solange er einer Konferenz nicht beigetreten ist, können die anderen Teilnehmer nur chatten. Sie können keine Vorführung anzeigen oder durchführen, weil der Konferenzleiter standardmäßig auch gleichzeitig ***Vorführende*** ist. Er (oder ein von ihm ernannter Teilnehmer) startet die Konferenzvorführung, indem er seinen Desktop oder einige Anwendungen für die anderen Teilnehmer freigibt. Nach der Freigabe durch den Vorführenden wird auf dem Desktop jedes Konferenzteilnehmers automatisch ein Konferenz-Betrachter geöffnet, in dem die freigegebenen Anwendungen des Vorführenden angezeigt werden.[1]

Der Konferenzleiter kann Teilnehmer ggf. auch von der Konferenz ausschließen, die Konferenz verlängern, falls die geplante Dauer überschritten wird, und die Konferenz beenden. Der Konferenzleiter kann seinen Verantwortungsbereich während einer Konferenz auf einen anderen Teilnehmer übertragen, wobei dieser in der richtigen Umgebung arbeiten muss. Er kann jeden anderen IVE-Benutzer als Konferenzleiter und jeden anderen Windows- oder Macintosh-Benutzer als Vorführenden einsetzen.

Der Vorführende kann auch Verantwortung an einen anderen Teilnehmer abgeben, indem er einen Steuernden bestimmt. Ein ***Steuernder*** verwendet seine eigene Maus und Tastatur zur Remotesteuerung des freigegebenen Desktops oder der freigegebenen Anwendungen des Vorführenden. Beachten Sie, dass der Vorführende die Berechtigung für die Remotesteuerung nicht nur IVE-Teilnehmern und Windows- oder Macintosh-Benutzern, sondern allen Teilnehmern erteilen kann. Wenn der Vorführende die Kontrolle über seine remotegesteuerten Anwendungen zurückerlangen möchte, muss er lediglich an einer beliebigen Stelle mit der Maustaste klicken, um die Steuerung von Secure Meeting wieder zurückzuerhalten.

1. Secure Meeting kann den Inhalt des Desktops des Vorführenden nicht anzeigen, wenn er gesperrt ist.

Von Secure Meeting unterstützte Umgebungen

Secure Meeting kann in verschiedenen Umgebungen eingesetzt werden, wie in der folgenden Tabelle erläutert. Für die Verwendung von Secure Meeting müssen IVE-Benutzer und andere Konferenzteilnehmer mit einem der unten angegebenen Betriebssysteme und Browser arbeiten und mindestens eine der Browserkomponenten aktivieren:

Betriebssysteme	Browser	Browserkomponenten[1]
Windows 98 SE Windows 2000 Windows NT 4.0 (SP 6)	Internet Explorer 5.0 Internet Explorer 5.5 (SP2) Internet Explorer 6.0 Netscape Navigator 7.1	Active-X MS JVM Sun JVM, Version 1.4.1_01 oder höher
Windows ME	Internet Explorer 5.5 (SP2) Internet Explorer 6.0 Netscape Navigator 7.1	Active-X MS JVM Sun JVM, Version 1.4.1_01 oder höher
Windows XP	Internet Explorer 6.0 Netscape Navigator 7.1	Active-X MS JVM Sun JVM, Version 1.4.1_01 oder höher
Mac OSX 10.2.8[2]	Safari 1.0	Sun JVM, Version 1.4.1_01 oder höher
Mac OSX 10.3.3[2]	Safari 1.2.1	Sun JVM, Version 1.4.1_01 oder höher
Linux RedHat 7.3[3]	Mozilla 1.6 Mozilla 1.3[4]	Sun JVM, Version 1.4.1_01 oder höher
Linux RedHat 9.0[3]	Mozilla 1.6[4]	Sun JVM, Version 1.4.1_01 oder höher

Betriebssysteme	Browser	Browserkomponenten[1]

1 Secure Meeting-Benutzer müssen nicht nur eine der hier aufgeführten Browserkomponenten, sondern auch JavaScript und Cookies aktivieren. Informationen zum Aktivieren von Browserkomponenten finden Sie in der Hilfe des entsprechenden Webbrowsers oder in der IVE-Endbenutzerhilfe im Thema über das Beitreten zu einer Konferenz.

2 Macintosh-Benutzer können ihren Desktop während einer Konferenz freigeben. Dies bezieht sich jedoch nicht auf einzelne Anwendungen. Beachten Sie außerdem, dass Macintosh-Benutzer über mindestens 256 MB Arbeitsspeicher verfügen müssen.

3 Benutzer von Linux können bei Konferenzen nicht Vorführende sein.

4 Secure Meeting wurde unter Mozilla 1.1.1 nicht getestet.

Zusätzlich zu der hier bereitgestellten Liste können Sie auch über die Secure Meeting-Kompatibilitätsprüfung ermitteln, ob Ihr System mit Secure Meeting kompatibel ist. Wechseln Sie hierfür zu jedem beliebigen Zeitpunkt mithilfe des Konferenz-URLs (`https://IhrIVE/Meeting`) oder der Konferenzeinladungs-E-Mails zur Konferenzanmeldeseite, und klicken Sie auf **Check Meeting Compatibility**. Secure Meeting ermittelt den Grad der Kompatibilität und schlägt zum Erreichen voller Kompatibilität ggf. Aktualisierungen vor. Beachten Sie jedoch, dass die Secure Meeting-Kompatibilitätsprüfung nicht alle Faktoren überprüft, die sich auf das Durchführen einer Konferenz auswirken können. Weitere System-anforderungen und Einschränkungen:

- Secure Meeting unterstützt keine Konferenzen in IVE-Umgebungen, die mit dem 2.x-Autorisierungsmodus des IVE konfiguriert sind (Legacymodus).
- Secure Meeting unterstützt keine Farbanzeige über 32-Bit auf dem Bildschirm (weiter Informationen finden Sie unter „Konfigurieren der Seite „Meetings““ auf Seite 517) oder Bildschirmauflösungen über 2048 x 2048 Pixel.
- Das Freigeben von Streamingmedien-Anwendungen wird von Secure nicht unterstützt.
- Wenn Sie Secure Meeting mit einem SSL-Zertifikat verwenden, empfiehlt es sich, auf Produktionsebene ein Zertifikat auf dem Secure Meeting-Server (d. h. dem IVE) zu installieren. Wenn Sie ein selbst signiertes SSL-Zertifikat installieren, können für Secure Meeting-Benutzer möglicherweise Schwierigkeiten bei der Konferenzanmeldung auftreten (siehe „Mehrere Serverzertifikate“ auf Seite 71). Wenn Sie ein selbst signiertes Zertifikat verwenden möchten, weisen Sie die Konferenzteilnehmer an, das Zertifikat vor dem Beitreten der Konferenz zu installieren. (In Internet Explorer klicken die Benutzer auf **Zertifikat**

anzeigen und dann auf **Zertifikat installieren**, wenn die Fehlermeldung angezeigt wird.)

Secure Meeting – Fehlerbehebung

Wenn bei Ihnen oder Endbenutzern Probleme mit Secure Meeting auftreten, empfehlen wir Folgendes:

- **Deinstallieren Sie den Secure Meeting-Client von Ihrem System**.

  Wenn beim Starten von Secure Meeting ein Problem auftritt, klicken Sie auf die Verknüpfung **Joining a Meeting: Troubleshooting** auf der Seite **Join Meeting**. Klicken Sie dann auf **Uninstall**. Klicken Sie auf **Return to Join Meeting**, und versuchen Sie erneut, die Konferenz zu starten. Beim nächsten Versuch, einer Konferenz beizutreten, aktualisiert Secure Meeting Ihren Client mit der aktuellen Version.

- **Überprüfen Sie die Systemkompatibilität**.

  Wenn Ihre Systemkonfiguration nicht mit Secure Meeting kompatibel ist, können beim Beitreten zu einer Konferenz oder bei der Vorführung Probleme auftreten. Sie ermitteln die Kompatibilität Ihres Systems, indem Sie zur Anmeldeseite für die Konferenz wechseln und auf **Check Meeting Compatibility** klicken.

- **Weitere Informationen können Sie der PDF-Datei Secure Meeting Error Messages entnehmen**.

  In der PDF-Datei *Secure Meeting Error Messages* sind Fehler aufgeführt, die beim Konfigurieren oder Verwenden von Secure Meeting auftreten können, und der Umgang mit diesen Fehlern wird erläutert. Die PDF-Datei ist auf der Juniper Networks-Supportsite verfügbar.

- **Wenden Sie sich an den Juniper Networks-Supportsite**.

  Wenn ein Fehler auftritt, den Sie mit den oben beschriebenen Verfahren nicht beheben können, senden Sie eine klare Beschreibung des Problems an den Juniper Networks-Supportsite. Geben Sie detailliert an, wie der Fehler und der Fehlermeldungstext nachzuvollziehen sind, und geben Sie Ihr IVE-Betriebssystem mit Buildnummer und Ihre IVE-Administratorprotokolldateien, Installationsprotokolldateien und Clientprotokolldateien an.

Zugreifen auf Client- und Installationsprotokolldateien

Abhängig von Ihren Berechtigungen und Ihrem Betriebssystem installiert Secure Meeting Clientdateien in unterschiedlichen Verzeichnissen. Beachten Sie, dass Sie die Clientprotokollierung über die Optionen in der Webkonsole auf der Registerkarte **System > Configuration > Security > Client-side Logs** deaktivieren können.

Windows-Benutzer mit Administrator- oder Hauptbenutzerberechtigungen suchen in:

- C:\Programme\Neoteris\Secure Meeting <Versionsnummer>\dsCboxUI.log
- C:\Windows -oder- WINNT\Übertragene Programmdateien\NeoterisSetup.log

Windows-Benutzer mit Standardberechtigungen suchen in[1]:

- C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\Neoteris\Secure Meeting <Versionsnummer>\dsCboxUI.log
- C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\Neoteris\Neoteris\NeoterisSetup.log -und- NeoterisSetupApp.log

Macintosh- und Linux-Benutzer suchen in: \tmp\dsCboxUI.log. Darüber hinaus sollten Macintosh- und Linux-Benutzer den Inhalt ihrer Java-Konsolen kopieren und in eine separate Datei einfügen, die an den Juniper Networks-Support gesendet wird.

Zugreifen auf Administratorprotokolle

Administratorprotokolle sind in der Webkonsole auf der Seite **System > Log/Monitoring** zu finden. Beachten Sie dabei, dass es drei Protokolle gibt: Ereignisprotokoll (Events Log), Benutzerzugriffsprotokoll (User Access Log) und Administratorzugriffsprotokoll (Administrator Access Log).

---

1. Benutzer ohne Administratorberechtigungen finden die Protokolldaten möglicherweise nicht, da sie verborgen sind. Sie aktivieren die Anzeige verborgener Dateien oder Ordner in Windows Explorer, indem Sie im Menü Extras die Option Ordneroptionen auswählen. Aktivieren Sie dann auf der Registerkarte Ansicht die Option Alle Dateien und Ordner anzeigen, und klicken Sie anschließend auf OK.

Zugriffsverwaltung – Übersicht

Das IVE ermöglicht es Ihnen, die Ressourcen Ihres Unternehmens mithilfe von Authentifizierungsrichtlinien, Benutzerprofilen und Ressourcenrichtlinien zu sichern. Mit diesen drei Kontrollstufen können Sie die Zugriffsverwaltung für das gesamte Unternehmen steuern. Sie können Sicherheitsanforderungen angeben, die Benutzer erfüllen müssen, um sich beim IVE anzumelden und auf IVE-Funktionen oder bestimmte URLs, Dateien und weitere Serverressourcen zugreifen zu können. Das IVE setzt die konfigurierten Richtlinien, Regeln und Einschränkungen sowie die Bedingungen durch, mit deren Hilfe die Benutzer daran gehindert werden, Verbindungen mit unautorisierten Ressourcen und Inhalten herzustellen oder diese herunterzuladen.

Weitere Informationen finden Sie unter:

Richtlinien, Regeln und Einschränkungen sowie Bedingungen

Der Zugriff auf Ressourcen beginnt im Authentifizierungsbereich. Als ***Authentifizierungsbereich*** wird eine Gruppierung von Authentifizierungsressourcen bezeichnet. Dies umfasst folgende Ressourcen:

- **Authentifizierungsserver** – Überprüfen die Identität des Benutzers. Das IVE leitet die Anmeldeinformationen eines Benutzers von der Anmeldeseite an einen Authentifizierungsserver weiter (Seite 283).
- **Authentifizierungsrichtlinien** – Geben die Sicherheitsanforderungen des Bereichs an, die erfüllt sein müssen, damit das IVE die Anmeldeinformationen eines Benutzers zur Überprüfung an einen Authentifizierungsserver weiterleitet (Seite 267).
- **Verzeichnisserver** – LDAP-Server, die dem IVE Benutzer- und Gruppeninformationen bereitstellen, mit denen das IVE Benutzer zu einer oder mehreren Benutzerrollen zuordnet (Seite 303).
- **Rollenzuordnungsregeln** – Geben die Bedingungen an, die ein Benutzer erfüllen muss, damit ihn das IVE zu einer oder mehreren Rollen zuweist. Diese Bedingungen beruhen entweder auf den Benutzerinformationen, die der Verzeichnisserver des Bereichs zurückgibt, oder auf dem Benutzernamen des Benutzers (Seite 382).

Einer IVE-Anmeldeseite sind ein oder mehrere Authentifizierungsbereiche zugeordnet. Wenn mehrere Bereiche für eine Anmeldeseite vorhanden sind,

muss der Benutzer vor der Übermittlung der Anmeldeinformationen einen Bereich angeben. Wenn der Benutzer die Anmeldeinformationen übermittelt hat, überprüft das IVE die Authentifizierungsrichtlinie des gewählten Bereichs. Der Benutzer muss die für die Authentifizierungsrichtlinien des Bereichs angegebenen Sicherheitsanforderungen erfüllen, andernfalls leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter.

Sie können auf Bereichsebene Sicherheitsanforderungen angeben, die auf folgenden Aspekten basieren: der Quell-IP des Benutzers, dem Browser, von dem aus der Zugriff auf das IVE erfolgt, der Besitz eines clientseitigen Zertifikats, die Länge des Benutzer-Kennwortes, ob die Hostprüfung installiert ist oder ob die Cachebereinigung auf dem Benutzercomputer installiert ist oder ausgeführt wird. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie für den Bereich erfüllt, leitet das IVE die Anmeldeinformationen des Benutzers an den entsprechenden Authentifizierungsserver weiter. Wenn der Benutzer durch den Server authentifiziert wurde, wertet das IVE die Rollenzuordnungsregeln für den Bereich aus und ermittelt, welche Rollen dem Benutzer zugeordnet werden.

Eine ***Rolle*** ist eine definierte Einheit, die die IVE-Sitzungseigenschaften für die Benutzer angibt, die der Rolle zugeordnet sind. Diese Sitzungseigenschaften enthalten Informationen wie Sitzungszeitbegrenzungen, Lesezeichen und aktivierte Zugriffsfunktionen – Webbrowsing, Dateinavigation, Secure Application Manager, Telnet/SSH, Network Connect, Secure Meeting und E-Mail-Client. Die Rollen-konfiguration bildet die zweite Ebene der Ressourcenzugriffssteuerung. Eine Rolle gibt nicht nur die Zugriffsmechanismen an, die einem Benutzer zur Verfügung stehen, sondern auch Beschränkungen, denen Benutzer entsprechen müssen, um einer Rolle zugeordnet werden zu können. Der Benutzer muss diese Sicherheitsanforderungen erfüllen, andernfalls ordnet ihn das IVE keiner Rolle zu.

Auf Rollenebene können Sie Sicherheitsanforderungen auf der Grundlage folgender Aspekte angeben: Quell-IP des Benutzers, Browser, Besitz eines clientseitigen Zertifikats, ob die Hostprüfung installiert ist oder bestimmte Richtlinien auf dem Benutzercomputer durchsetzt und ob die Cachebereinigung auf dem Benutzercomputer ausgeführt wird. Wenn der Benutzer die Anforderungen erfüllt, die von einer Rollenzuordnungsregel oder den Einschränkungen einer Rolle[1] angegeben sind, ordnet das IVE den Benutzer zu einer Rolle zu. Wenn ein Benutzer eine Anforderung an die für die Rolle verfügbaren Back-End-Ressourcen sendet, wertet das IVE die entsprechenden Ressourcenrichtlinien für die Zugriffsfunktion aus.

Eine ***Ressourcenrichtlinie*** ist eine Reihe von Ressourcennamen (wie URLs, Hostnamen und Kombinationen aus IP-Adresse und Netzmaske), denen der Zugriff oder die Ausführung anderer ressourcenspezifischer Aktionen wie Neuschreiben oder Zwischenspeicherung gewährt oder verweigert wird.

Eine Ressourcenrichtlinie bildet die dritte Ebene der Ressourcenzugriffssteuerung. Eine Rolle gewährt den Zugriff auf bestimmte Funktionen und Ressourcen (wie Lesezeichen und Anwendungen), wohingegen eine Ressourcenrichtlinie den Benutzerzugriff auf eine bestimmte Ressourcen steuert. Mithilfe dieser Richtlinien können sogar Bedingungen angegeben werden, die, sofern erfüllt, den Benutzerzugriff auf eine Serverfreigabe oder Datei verweigern oder gewähren. Derartige Bedingungen können auf den von Ihnen angegebenen Sicherheitsanforderungen basieren. Der Benutzer muss diese Sicherheitsanforderungen erfüllen, andernfalls wird die Benutzeranforderung vom IVE nicht verarbeitet.

Auf Ressourcenebene können Sie Sicherheitsanforderungen auf der Grundlage folgender Aspekte angeben: Quell-IP des Benutzers, Browser, Besitz eines clientseitigen Zertifikats, Tageszeit der Anforderung, ob die Hostprüfung installiert ist oder bestimmte Richtlinien auf dem Benutzercomputer durchsetzt und ob die Cachebereinigung auf dem Benutzercomputer installiert ist oder ausgeführt wird. Wenn der Benutzer die Anforderungen erfüllt, die in den Bedingungen einer Ressourcenrichtlinie angegeben sind, verweigert oder gewährt das IVE den Zugriff auf die angeforderte Ressource. Sie können z. B. Webzugriff auf Rollenebene aktivieren, sodass ein der Rolle zugewiesener Benutzer eine Webanforderung ausführen kann. Sie können auch eine Webressourcenrichtlinie so konfigurieren, dass Anforderungen an einen bestimmten URL oder Pfad verweigert werden, wenn die Hostprüfung auf dem Benutzercomputer eine inakzeptable Datei findet. In diesem Szenario überprüft das IVE, ob die Hostprüfung ausgeführt wird, und gibt dann an, dass der Benutzercomputer der erforderlichen Hostprüfung-Richtlinie entspricht. Wenn dies der Fall ist, d. h. die inakzeptable Datei nicht gefunden wurde, gewährt das IVE dem Benutzer Zugriff auf die angeforderte Webressource.

1. Sicherheitsanforderungen für eine Rolle können an zwei Positionen angegeben werden: in den Rollenzuordnungsregeln eines Authentifizierungsbereichs (mit benutzerdefinierten Ausdrücken) oder durch die Angabe von Einschränkungen in der Rollendefinition. Das IVE wertet die angegebenen Anforderungen an beiden Positionen aus. Dies gewährleistet, dass nur Benutzer einer Rolle zugeordnet werden, die die Anforderungen erfüllen.

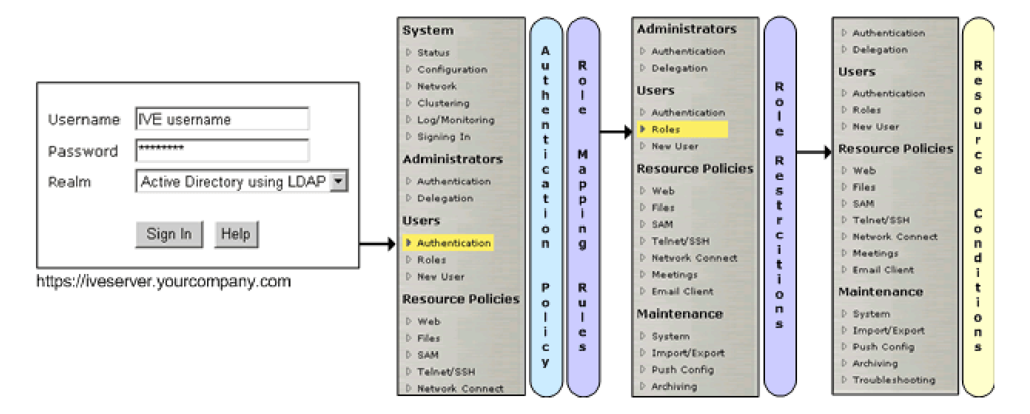


Abbildung 2: Zugriffsverwaltung
In dieser Abbildung ist die Reihenfolge dargestellt, in der das IVE Richtlinien, Regeln, Einschränkungen und Bedingungen auswertet, nachdem ein Benutzer seine Anmeldeinformationen auf der Anmeldeseite übermittelt hat.

Angeben von Sicherheitsanforderungen

Mit dem IVE können Sicherheitsanforderungen für Administratoren und Benutzer ganz einfach über die folgenden Optionen und Funktionen angegeben werden:

Quell-IP

Sie können den Zugriff auf das IVE und die Ressourcen anhand der Quell-IP einschränken.

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Computer anmelden, dessen Kombination aus IP-Adresse und Netzmaske den angegebenen Quell-IP-Anforderungen für den ausgewählten Authentifizierungsbereich entspricht. Verfügt der Benutzercomputer nicht über eine für den Bereich erforderliche Kombination aus IP-Adresse und Netzmaske, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und dem Benutzer wird der Zugriff auf das IVE verweigert.

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer aus anmelden, dessen Kombination aus IP-Adresse und Netzmaske den angegebenen Quell-IP-Anforderungen für jede der Rollen entspricht, zu denen das IVE den Benutzer zuordnet. Verfügt der Benutzercomputer nicht über eine Kombination aus IP-Adresse und Netzmaske, die für eine Rolle erforderlich ist, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur von einem Computer durchführen, dessen Kombination aus IP-Adresse und Netzmaske den im Zusammenhang mit der Benutzeranforderung angegebenen Quell-IP-Anforderungen für die Ressourcenrichtlinie entspricht. Verfügt der Benutzercomputer nicht über die erforderliche Kombination aus IP-Adresse und Netzmaske, die für eine Ressource erforderlich ist, gewährt das IVE dem Benutzer keinen Zugriff auf die Ressource.

Browser

Sie können den Zugriff auf das IVE und auf Ressourcen anhand des Browsertyps einschränken.

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Browser anmelden, dessen Benutzer-Agent-Zeichenfolge dem Zeichenfolgenmuster entspricht, das für den ausgewählten Authentifizierungsbereich angegeben wurde. Wenn die Benutzer-Agent-Zeichenfolge des Browsers für den Bereich zulässig ist, leitet das IVE die Anmeldeinformationen an den Authentifizierungsserver weiter. Wenn die Benutzer-Agent-Zeichenfolge des Browsers nicht für den Bereich zulässig ist, leitet das IVE die Anmeldeinformationen nicht an den Authentifizierungsserver weiter.

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Browser anmelden, dessen Benutzer-Agent-Zeichenfolge den jeweils angegebenen Zeichenfolgenmustern für die einzelnen Rollen entspricht, denen der Benutzer durch das IVE zugeordnet werden kann. Wenn die Benutzer-Agent-Zeichenfolge nicht den Zulassungsanforderungen für eine Rolle entspricht, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur von einem Browser durchführen, dessen Benutzer-Agent-Zeichenfolge mit den Zulassungsanforderungen für die Ressourcenrichtlinie übereinstimmt, die für die Benutzeranforderung gilt. Wenn die Benutzer-Agent-Zeichenfolge nicht den Zulassungsanforderungen für eine Ressource entspricht, verweigert das IVE dem Benutzer den Zugriff auf die Ressource.

Zertifikat

Sie können den Zugriff auf das IVE und die Ressourcen durch Anforderung clientseitiger Zertifikate einschränken:

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer kann sich nur von einem Computer anmelden, der das angegebene clientseitige Zertifikat besitzt (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare). Wenn der Benutzercomputer nicht über die für den Bereich erforderlichen Zertifikatinformationen verfügt, kann der Benutzer auf die Anmeldeseite zugreifen, doch sobald vom IVE festgestellt wird, dass der Benutzerbrowser das Zertifikat nicht besitzt, werden die Anmeldeinformationen des Benutzers vom IVE nicht an den Authentifizierungsserver übermittelt, sodass der Benutzer nicht auf die Funktionen des IVE zugreifen kann.

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer anmelden, der die angegebenen Anforderungen des clientseitigen Zertifikats (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare) für jede der Rollen erfüllt, zu der das IVE den Benutzer zuordnet. Besitzt der Benutzercomputer nicht die Zertifikatinformationen, die für eine Rolle erforderlich sind, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer muss eine Ressourcenanforderung von einem Computer ausführen, der die angegebenen Anforderungen des clientseitigen Zertifikats (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare) für die Ressourcenrichtlinie erfüllt, die für die Benutzeranforderung angegeben wurde. Besitzt der Benutzercomputer nicht die Zertifikatinformationen, die für eine Ressource erforderlich sind, verweigert das IVE dem Benutzer den Zugriff auf die Ressource.

Kennwort

Sie können den Zugriff auf das IVE und auf Ressourcen anhand der Kennwortlänge einschränken.

Bei Anmeldung von Administratoren oder Benutzern am IVE.

Der Benutzer muss ein Kennwort eingeben, das der Mindestkennwortlänge entspricht, die für den Bereich angegeben wurde. Beachten Sie, dass die Datensätze für lokale Benutzer und Administratoren auf dem IVE-Authentifizierungsserver gespeichert werden. Auf diesem Server müssen Kennwörter mindestens 6 Zeichen lang sein, unabhängig von dem Wert, der für die Authentifizierungs-richtlinie des Bereichs angegeben wurde.

Hostprüfung

Sie können den Zugriff auf das IVE und die Ressourcen durch Anforderung der Hostprüfung einschränken:

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Computer anmelden, der den Hostprüfung-Richtlinien entspricht, die für den Bereich angegeben wurden. Wenn der Benutzercomputer den Anforderungen der Richtlinien für die Hostprüfung nicht entspricht, die für den Bereich angegeben wurden, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und dem Benutzer wird der Zugriff auf das IVE verweigert.

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer anmelden, der den Hostprüfung-Richtlinien für jede der Rollen entspricht, zu denen das IVE den Benutzer zuordnet. Wenn der Benutzercomputer die Anforderungen der Hostprüfung-Richtlinien nicht erfüllt, die für eine Rolle angegeben wurden, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur von einem Computer ausführen, der den Hostprüfung-Richtlinien für die Ressourcenrichtlinie entspricht, die für die Benutzeranforderung gilt. Wenn der Benutzercomputer die Anforderungen der Hostprüfung-Richtlinien nicht erfüllt, die für eine Ressource angegeben wurden, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

Cachebereinigung

Sie können den Zugriff auf das IVE und die Ressourcen durch Anforderung der Cachebereinigung einschränken:

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Computer anmelden, der den Cachebereinigung-Richtlinien entspricht, die für den Bereich angegeben wurden. Wenn der Benutzercomputer den Anforderungen der Richtlinien für die Cachebereinigung nicht entspricht, die für den Bereich angegeben wurden, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und dem Benutzer wird der Zugriff auf das IVE verweigert.

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer anmelden, der der Anforderung für die Cachebereinigung entspricht, die für jede der Rollen angegeben wurde, zu der das IVE den Benutzer zuordnet. (Dabei muss die Cachebereinigung, je nach Konfiguration, auf der Arbeitsstation ausgeführt oder ggf. installiert werden.) Wenn der Benutzercomputer die Anforderungen für die Cachebereinigung, die für eine Rolle angegeben wurden, nicht erfüllt, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer muss sich von einem Computer anmelden, der der Anforderung an die Cachebereinigung für die Ressourcenrichtlinien entspricht, die für die Anforderung des Benutzers gültig ist. (Dabei muss die Cachebereinigung, je nach Konfiguration, auf der Arbeitsstation ausgeführt oder ggf. installiert werden.) Wenn der Benutzercomputer die Anforderung an die Cachebereinigung nicht erfüllt, die für eine Ressource angegeben wurde, gewährt das IVE dem Benutzer keinen Zugriff auf die Ressource.

Authentifizierungsbereiche – Übersicht

Als ***Authentifizierungsbereich*** wird eine Gruppierung von Authentifizierungsressourcen bezeichnet. Dies umfasst folgende Ressourcen:

- **Authentifizierungsserver** – Überprüfen die Identität des Benutzers. Das IVE leitet die Anmeldeinformationen eines Benutzers von der Anmeldeseite an einen Authentifizierungsserver weiter (Seite 35).
- **Authentifizierungsrichtlinien** – Geben die Sicherheitsanforderungen des Bereichs an, die erfüllt sein müssen, damit das IVE die Anmeldeinformationen eines Benutzers zur Überprüfung an einen Authentifizierungsserver weiterleitet (Seite 37).
- **Verzeichnisserver** – LDAP-Server, die dem IVE Benutzer- und Gruppeninformationen bereitstellen, mit denen das IVE Benutzer zu einer oder mehreren Benutzerrollen zuordnet (Seite 37).
- **Rollenzuordnungsregeln** – Geben die Bedingungen an, die ein Benutzer erfüllen muss, damit ihn das IVE zu einer oder mehreren Rollen zuweist. Diese Bedingungen beruhen entweder auf den Benutzerinformationen, die der Verzeichnisserver des Bereichs zurückgibt, oder auf dem Benutzernamen des Benutzers (Seite 38).

Authentifizierungsserver

Bei einem ***Authentifizierungsserver*** handelt es sich um eine Datenbank, in der Anmeldeinformationen für Benutzer (Benutzername und Kennwort) und normalerweise Gruppeninformationen gespeichert werden. Wenn sich ein Benutzer am IVE anmeldet, gibt er einen Authentifizierungsbereich an, der einem Authentifizierungsserver zugeordnet ist. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie erfüllt, leitet das IVE die Anmeldeinformationen des Benutzers an den zugeordneten Authentifizierungsserver weiter. Der Authentifizierungsserver überprüft das Vorhandensein und die Identität der Benutzer. Anschließend sendet der Authentifizierungsserver die Bestätigung und, wenn der Server in dem Bereich auch als Verzeichnis-/Attributserver verwendet wird, auch die Gruppeninformationen des Benutzers oder andere Benutzerattributinformationen an das IVE. Das IVE ermittelt die Rollenzuordnungsregeln für den Bereich und die Benutzerrollen, denen ein Benutzer zugeordnet werden kann.

Zum Angeben eines Authentifizierungsservers, der für einen Bereich verwendet werden kann, müssen Sie zunächst auf der Seite **System > Signing In > Servers** eine Serverinstanz konfigurieren. Wenn Sie die Servereinstellungen speichern, wird der Servername (der der Instanz zugewiesene Name) auf der Registerkarte **General** des Bereichs in der Dropdownliste **Authentication Server** angezeigt. Wenn es sich beim Server um einen LDAP- oder Active Directory-Server handelt, wird auch der Name der Instanz auf der Registerkarte **General** des Bereichs in der Dropdownliste **Directory/Attribute server** angezeigt. Sie können denselben LDAP- oder Active Directory-Server in einem Bereich für Authentifizierung und Autorisierung verwenden, oder Sie verwenden dieselbe Serverinstanz zur Authentifizierung in einem Bereich und zur Autorisierung in verschiedenen anderen Bereichen, in denen andere Server zur Authentifizierung verwendet werden.

Das NetScreen Instant Virtual Extranet unterstützt die gängigsten Authentifizierungsserver, z. B. Windows NT-Domäne, Active Directory, RADIUS, LDAP, NIS, RSA ACE/Server und Netegrity SiteMinder. Sie können eine oder mehrere lokale Datenbanken für vom IVE authentifizierte Benutzer erstellen. Eine Übersicht über Server und Informationen zur Konfiguration finden Sie unter:

Hinweis: Ein Authentifizierungsserver muss eine Verbindung mit dem IVE-Server herstellen können. Wenn ein Authentifizierungsserver wie RSA ACE/Server keine IP-Adressen für die Agentenhosts verwendet, muss er den IVE-Hostnamen über einen DNS-Eintrag oder einen Eintrag in der eigenen Hostdatei auflösen können.

Authentifizierungsrichtlinien

Eine ***Authentifizierungsrichtlinie*** besteht aus einer Reihe von Regeln für einen Aspekt der Zugriffsverwaltung, die steuern, ob dem Benutzer eine Anmeldeseite für den Bereich angezeigt wird. Eine Authentifizierungsrichtlinie ist Bestandteil der Konfiguration eines Authentifizierungsbereichs. Sie gibt die Regeln für das IVE an, die vor dem Anzeigen einer Anmeldeseite berücksichtigt werden müssen. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie für den Bereich erfüllt, zeigt das IVE dem Benutzer die Anmeldeseite an und leitet die Anmeldeinformationen des Benutzers an den entsprechenden Authentifizierungsserver weiter. Wenn der Benutzer durch den Server authentifiziert wird, beginnt das IVE mit der Rollenauswertung.

Verzeichnisserver

Ein ***Verzeichnisserver*** ist eine Datenbank, in der Benutzer- und meistens Gruppeninformationen gespeichert werden. Sie können einen Authentifizierungsbereich so konfigurieren, dass ein Verzeichnisserver Benutzer- oder Gruppeninformationen abruft, die in Rollenzuordnungsregeln und Ressourcenrichtlinien verwendet werden. Gegenwärtig unterstützt das IVE hierfür LDAP-Server, ein LDAP-Server kann daher zur Authentifizierung und Autorisierung verwendet werden. Sie müssen nur eine Serverinstanz definieren, dann wird der Name der LDAP-Serverinstanz in den Dropdownlisten **Authentication Server** und **Directory/Attribute Server** auf der Registerkarte **General** des Bereichs angezeigt. Sie können denselben Server für eine unbeschränkte Anzahl von Bereichen verwenden.

Neben einem LDAP-Server können Benutzerattribute auch mit einem RADIUS-Server abgerufen werden, um sie in Rollenzuordnungsregeln zu verwenden. Eine RADIUS-Serverinstanz wird jedoch im Gegensatz zu einer LDAP-Serverinstanz nicht in den Dropdownlisten des Bereichs und von **Directory/Attribute Server** angezeigt. Um einen RADIUS-Server zum Abrufen von Benutzerinformationen zu verwenden, müssen Sie nur seine Instanz in der Liste **Authentication Server** angeben und dann in der Liste **Directory/Attribute server** die Option **None** auswählen. Dann konfigurieren Sie Rollenzuordnungsregeln, um Attribute des RADIUS-Servers zu verwenden, die in einer Attributliste auf der Seite **Role Mapping Rule** verfügbar sind, nachdem **Rule based on User attribute** ausgewählt wurde.

Weitere Informationen zum Angeben eines Verzeichnisservers finden Sie unter „Erstellen eines Authentifizierungsbereichs“ auf Seite 379. Weitere Informationen zum Angeben von LDAP- oder RADIUS-Attributen in Rollenzuordnungsregeln finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 382.

Rollenzuordnungsregeln

Eine ***Rollenzuordnungsregel*** ist eine Anweisung, die in folgendem Format angegeben wird:

Wenn die angegebene Bedingung wahr|nicht wahr ist, dann ordne den Benutzer den ausgewählten Rollen zu.

Sie erstellen eine Rollenzuordnungsregel auf der Registerkarte **Role Mapping**[1] eines Authentifizierungsbereichs. Wenn Sie auf dieser Registerkarte auf **New Rule** klicken, wird die Seite **Role Mapping Rule** angezeigt. Sie enthält einen integrierten Editor für die Definition von Regeln. Der Editor führt Sie durch die drei Schritte, die zum Erstellen einer Regel notwendig sind:

1. Geben Sie den Bedingungstyp an, auf dem die Regel beruhen soll. Folgende Optionen stehen zur Verfügung:
   - Benutzername
   - Benutzerattribut
   - Zertifikat oder Zertifikatsattribut
   - Gruppenmitgliedschaft
   - Benutzerdefinierte Ausdrücke
2. Geben Sie die auszuwertende Bedingung an, die sich folgendermaßen zusammensetzt:
   1. Angeben von einem oder mehreren Benutzernamen, Benutzerattributen, Zertifikatsattributen, Gruppen (LDAP) oder Ausdrücken, die von dem in Schritt 1 ausgewählten Bedingungstyp abhängen.
   2. Angeben der Wertentsprechungen. Dies kann auch eine Liste von IVE-Benutzernamen, Benutzerattributswerten von einem RADIUS- oder LDAP-Server, clientseitigen Zertifikatswerten (statisch oder im Vergleich mit LDAP-Attributen), LDAP-Gruppen oder vordefinierten Ausdrücken umfassen.
3. Geben Sie die Rollen an, die dem authentifizierten Benutzer zugewiesen werden sollen.

---

1. Administratoren erstellen Rollenzuordnungsregeln auf der Registerkarte **Administrators > Authentication >** *Ausgewählter Bereich* **> Role Mapping**. Benutzer erstellen Rollenzuordnungsregeln auf der Registerkarte **Users > Authentication >** *Ausgewählter Bereich* > **Role Mapping**.

Das IVE stellt eine Liste aller ***zulässigen Rollen*** zusammen, denen ein Benutzer zugeordnet werden kann. Diese Rollen ergeben sich aus den Rollenzuordnungsregeln, denen ein Benutzer entspricht. Anschließend wertet das IVE die Definitionen der einzelnen Rollen aus, um festzustellen, ob der Benutzer Rolleneinschränkungen unterliegt. Das IVE erstellt anhand dieser Informationen eine Liste der ***gültigen Rollen***, d. h. der Rollen, für die der Benutzer zusätzliche Anforderungen erfüllt. Abschließend führt das IVE entweder eine permissive Zusammenführung der gültigen Rollen durch oder zeigt dem Benutzer eine Liste gültiger Rollen an. Dies hängt von der Konfiguration ab, die auf der Registerkarte **Role Mapping** des Bereichs angegeben ist.

Weitere Informationen über Rollen finden Sie unter „Benutzerrollen – Übersicht“ auf Seite 55. Weitere Informationen über das Angeben von Rollenzuordnungsregeln finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 382.

Ressourcenrichtlinien – Übersicht

Eine ***Ressourcenrichtlinie*** ist eine Richtlinie, die Ressourcen und Aktionen für eine bestimmte Zugriffsfunktion angibt. Eine Ressource kann entweder ein Server oder eine Datei sein, auf die über das IVE zugegriffen werden kann. Mithilfe einer Aktion wird einer Ressource „erlaubt" oder „verboten", eine Funktion durchzuführen. Jede Zugriffsfunktion verfügt über mindestens einen Richtlinientyp, der die Antwort des IVE auf eine Benutzeranfrage oder die Art bestimmt, wie eine Zugriffsfunktion aktiviert wird (im Fall von Secure Meeting und E-Mail-Client). Sie können auch detaillierte Regeln für eine Ressourcenrichtlinie definieren, mit denen Sie zusätzliche Anforderungen für bestimmte Benutzeranforderungen auswerten können.

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

Typen von Ressourcenrichtlinien

- **Webressourcenrichtlinien** – Die Webzugriffsfunktion verfügt über die folgenden Typen von Ressourcenrichtlinien:
  - Access: Gibt Webressourcen an, zu denen Benutzer navigieren bzw. nicht navigieren dürfen (Seite 446)
  - Caching: Gibt an, für welche Webressourcen das IVE Seitenheader sendet oder ändert (Seite 448)
  - Java Access: Gibt die Server an, mit denen Java-Applets eine Verbindung herstellen können (Seite 453)
  - Java Signing: Gibt an, ob Java-Applets mit einem Appletzertifikat oder dem Standard-IVE-Zertifikat neu signiert werden (Seite 454)
  - Selective Rewriting: Gibt an, welche Ressourcen das IVE neu schreiben kann (Seite 456)
  - Pass through Proxy: Gibt Webanwendungen an, für die das IVE eine minimale Vermittlung durchführt (Seite 458)
  - Form POST: Gibt an, ob die IVE-Anmeldeinformationen eines Benutzers direkt an ein Anmeldeformular einer Back-End-Webanwendung gesendet werden (Seite 460)
  - Cookies/Headers: Gibt an, ob Cookies und Header an ein Anmeldeformular einer Back-End-Webanwendung gesendet werden (Seite 462)

- **Dateiressourcenrichtlinien** – Die Dateizugriffsfunktion verfügt über die folgenden Typen von Ressourcenrichtlinien:
  - Windows Access: Gibt Windows-Dateiressourcen an, zu denen Benutzer navigieren bzw. nicht navigieren dürfen (Seite 483)
  - Windows Credentials: Gibt Windows-Dateiressourcen an, für die Sie oder Benutzer zusätzliche Anmeldeinformationen angeben müssen (Seite 486)
  - UNIX/NFS Access: Gibt UNIX/NFS-Dateiressourcen an, zu denen Benutzer navigieren bzw. nicht navigieren dürfen (Seite 489)
- **Secure Application Manager-Ressourcenrichtlinien** – Die Secure Application Manager-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinie: Diese erlaubt oder verweigert Anwendungen, die zum Verwenden von J-SAM oder W-SAM konfiguriert sind, die Herstellung von Socketverbindungen (Seite 496)
- **Telnet/SSH-Ressourcenrichtlinien** – Die Telnet/SSH-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinie: Diese erlaubt oder verweigert den Zugriff auf die angegebenen Server (Seite 503)
- **Network Connect-Ressourcenrichtlinien** – Die Network Connect-Zugriffsfunktion verfügt über zwei Typen von Ressourcenrichtlinien: Diese erlaubt oder verweigert den Zugriff auf die angegebenen Server und gibt IP-Adresspools an (Seite 509)
- **Secure Application Manager-Ressourcenrichtlinien** – Die Secure Application Manager-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinie: Diese aktiviert oder deaktiviert E-Mail-Benachrichtigungen an Benutzer, die zu einer Secure Meeting-Konferenz eingeladen wurden (Seite 517)
- **Secure Email Client-Ressourcenrichtlinien** – Die Secure Email Client-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinie: Diese aktiviert oder deaktiviert E-Mail-Client-Unterstützung (Seite 520)

Bestandteile einer Ressourcenrichtlinie

Eine Ressourcenrichtlinie enthält die folgenden Informationen:

- **Ressourcen:** Eine Reihe von Ressourcennamen (URLs, Hostnamen oder Kombinationen aus IP-Adresse/Netzmaske), die die Ressourcen angeben, für die die Richtlinie gilt. Sie können eine Ressource mit einem Platzhalterpräfix angeben, das für einen Hostnamen steht. Die Standardressource für eine Richtlinie wird durch ein Sternchen (*) angegeben, d. h., die Richtlinie gilt für alle entsprechenden Ressourcen. Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 45.

- **Rollen:** Eine optionale Liste von Benutzerrollen, für die diese Richtlinie gilt. Standardmäßig gilt die Richtlinie für alle Rollen.
- **Aktion:** Die Aktion, die das IVE durchführt, wenn ein Benutzer die Ressource entsprechend der Liste **Ressource** anfordert. Eine Aktion kann angeben, ob der Zugriff auf eine Ressource erlaubt oder verboten ist oder ob eine Aktion durchgeführt wird (z. B. das Neuschreiben von Webinhalt oder das Zulassen von Java-Socketverbindungen).
- **Detaillierte Regeln:** Eine optionale Liste von Elementen, die Ressourcendetails angibt (z. B. bestimmte URLs, Verzeichnispfade, Dateien oder Dateitypen), auf die eine andere Aktion angewendet werden soll oder für die vor der Anwendung der Aktion Bedingungen ausgewertet werden sollen. Sie können eine oder mehrere Regeln definieren und die Reihenfolge angeben, in der das IVE diese auswertet. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

Auswerten von Ressourcenrichtlinien

Wenn das IVE eine Benutzeranforderung erhält, wertet es die dem Anforderungstyp entsprechenden Ressourcenrichtlinien aus. Beim Verarbeiten der Richtlinie, die der angeforderten Ressource entspricht, führt es die angegebene Aktion für die Anforderung aus. Diese Aktion ist auf der Registerkarte **General** oder **Detailed Rules** der Richtlinie festgelegt. Wenn ein Benutzer beispielsweise eine Webseite anfordert, „weiß“ das IVE, wie die Webressourcenrichtlinien zu verwenden sind. Im Fall von Webanforderungen startet das IVE immer mit den Richtlinien für „Web Rewriting“ (Neuschreiben von Webinhalt), „Selective Rewriting“ (selektives Neuschreiben) und „Pass Through Proxy“ (Durchgangsproxy), um zu bestimmen, ob die Anforderung verarbeitet werden soll. Wenn keine dieser Richtlinien angewendet werden kann (oder keine definiert ist), wertet das IVE die Richtlinien für „Web Access“ (Webzugriff) aus, bis es eine findet, die zur angefragten Ressource gehört.

Das IVE wertet eine Gruppe von Ressourcenrichtlinien für eine Zugriffsfunktion von oben nach unten aus, d. h., es startet mit der ersten Richtlinie und durchläuft dann die Liste, bis eine passende Richtlinie gefunden wird. Wenn Sie detaillierte Regeln für die passende Richtlinie definiert haben, wertet das IVE die Regeln von oben nach unten aus und stoppt, wenn es in der Liste **Resource** der Regel eine passende Ressource findet. In der folgenden Abbildung werden die allgemeinen Schritte der Richtlinienauswertung dargestellt:

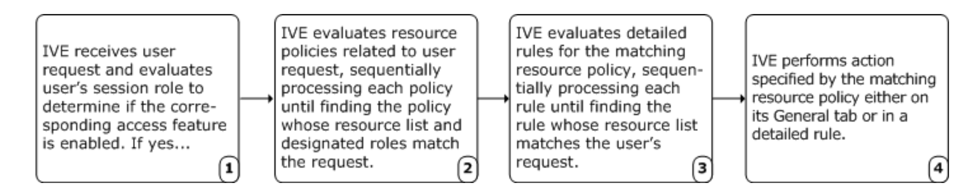


Abbildung 3: Schritte bei der Auswertung von Ressourcenrichtlinien

Details der einzelnen Auswertungsschritte:

1. Die „Sitzungsrolle" eines Benutzers beruht auf der Rolle bzw. den Rollen, der bzw. denen er während des Authentifizierungsvorgangs zugewiesen wird. Die für einen Benutzer aktivierten Zugriffsfunktionen werden durch eine Rollenzuordnungskonfiguration des Authentifizierungsbereichs bestimmt.
2. Die Funktionen für Web- und Dateizugriff verfügen über mehrere Typen von Ressourcenrichtlinien. Das IVE ermittelt daher zunächst den Anforderungstyp (z. B. auf eine Webseite, ein Java-Applet oder eine UNIX-Datei) und wertet dann die der Anforderung entsprechenden Ressourcenrichtlinien aus. Für die Webzugriffsfunktion werden z. B. für jede Webanforderung zuerst die Richtlinien zum Neuschreiben ausgewertet. Die verbleibenden fünf Zugriffsfunktionen, Secure Application Manager, Secure Terminal Access, Secure Meeting und Secure Email Client, verfügen über nur eine Ressourcenrichtlinie.
3. Mit einer detaillierten Regel können die folgenden beiden Vorgänge durchgeführt werden:
   - Ressourcen, für die eine Aktion gilt, können auf einer genaueren Ebene angegeben werden. Wenn Sie z. B. in den Hauptrichtlinien-Einstellungen einer Webzugriffs-Ressourcenrichtlinie einen Webserver angeben, können Sie eine detaillierte Regel definieren, die einen bestimmte Pfad auf diesem Server angibt, und dann die Aktion für diesen Pfad ändern.
   - Es kann vom Benutzer verlangt werden, dass er zum Anwenden der Aktion bestimmte Bedingungen erfüllt, die in Form boolescher Ausdrücke oder benutzerdefinierter Ausdrücke geschrieben wurden. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52).
4. Das IVE beendet die Verarbeitung von Ressourcenrichtlinien, sobald die angeforderte Ressource in der Liste **Resource** einer Richtlinie oder in einer detaillierten Regel gefunden wird.

Angeben von Ressourcen für eine Ressourcenrichtlinie

Für das IVE-Modul, dass Ressourcenrichtlinien auswertet, müssen die in der Liste **Resources** einer Richtlinie aufgelisteten Ressourcen im kanonischen Format aufgeführt sein. In diesem Abschnitt werden die kanonischen Formate beschrieben, die zum Angeben von Web-, Datei- und Serverressourcen verfügbar sind. Wenn ein Benutzer versucht, auf eine bestimmte Ressource zuzugreifen, vergleicht das IVE die angeforderte Ressource mit der in den entsprechenden Richtlinien angegebenen Ressource. Es beginnt dabei mit der ersten Richtlinie in der Richtlinienliste. Wenn das Modul eine angeforderte Ressource mit einer in der Liste **Resources** einer Richtlinie angegebenen Ressource abgleicht, wertet es weitere Richtlinieneinschränkungen aus und gibt die entsprechende Aktion an das IVE zurück (es werden keine weiteren Richtlinien ausgewertet). Wenn keine Richtlinie zutrifft, wertet das IVE Lesezeichen für automatische Erlaubnis (sofern definiert) aus, andernfalls wird die Standardaktion für die Richtlinie zurückgegeben.

Die erforderlichen kanonischen Formate werden in folgenden Abschnitten beschrieben:

- Angeben von Webressourcen (46)
- Angeben von Windows-Dateiressourcen (48)
- Angeben von UNIX/NFS-Dateiressourcen (49)
- Angeben von Serverressourcen (50)
- Angeben von IP-Adresspools (51)

Allgemeine Anmerkungen zu kanonischen Formaten

- Wenn eine Pfadkomponente mit einem Schrägstrich und einem Sternchen endet (/*), entspricht dies dem untergeordneten Knoten und allen weiteren Unterverzeichnissen. Wenn eine Pfadkomponente mit einem Schrägstrich und einem Prozentzeichen endet (/%), entspricht dies dem untergeordneten Knoten und allen Elementen, die sich genau einer Ebene darunter befinden.

  Beispiel:

  /intranet/* entspricht Folgendem:

  /intranet

  /intranet/home.html

  /intranet/elee/public/index.html

  /intranet/% entspricht Folgendem:

  /intranet

/intranet/home.html

aber nicht /intranet/elee/public/index.html

- Der Hostname und die IP-Adresse einer Ressource werden gleichzeitig an das Richtlinienmodul weitergegeben. Wenn ein Server in der Liste **Resources** einer Richtlinie als IP-Adresse angegeben ist, erfolgt die Auswertung anhand der IP-Adresse. Andernfalls versucht das Modul, die beiden Hostnamen abzugleichen. Es führt kein Reverse-DNS-Lookup zur Ermittlung der IP-Adresse durch.
- Wenn ein Hostname in der Liste **Resources** einer Richtlinie nicht vollständig qualifiziert ist, wenn z. B. „juniper" anstelle von „intranet.juniper.net" angegeben ist, führt das Modul die Auswertung anhand der vorliegenden Angaben durch, der Hostname wird nicht weiter qualifiziert.

Angeben von Webressourcen

Kanonisches Format: `[Protokoll://]Host[:Ports][/Pfad]`

Die vier Bestandteile sind:

- **Protokoll** (optional)

  Mögliche Werte: `http` und `https` (Groß- oder Kleinschreibung wird nicht berücksichtigt)

  Wenn das Protokoll fehlt, werden sowohl `http` als auch `https` angenommen. Bei der Eingabe eines Protokolls muss das Trennzeichen „`://`" eingegeben werden. Sonderzeichen sind nicht zulässig.

- **Host** (erforderlich)

  Mögliche Werte:

  - **DNS-Hostname**

    Beispiel: www.juniper.com

    Sonderzeichen sind zulässig, einschließlich:

*****	Entspricht ALLEN Zeichen
%	Entspricht einem beliebigen Zeichen außer dem Punkt (.)
?	Entspricht genau einem Zeichen

- **IP-Adresse/Netzmaske**

  Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`

  Die Netzmaske kann eins der beiden Formate aufweisen:

  - Präfix: Obere Bits
  - IP: `a.b.c.d`

  Beispiel: `10.11.149.2/24` oder `10.11.149.2/255.255.255.0`

  Sonderzeichen sind nicht zulässig.

- **Ports** (optional)

  Mögliche Werte:

*****	Entspricht ALLEN Ports, andere Sonderzeichen sind nicht zulässig.
Port[,Port]*	Eine durch Kommas getrennte Liste einzelner Ports. Gültige Portnummern sind [1-65535].
[Port 1]-[Port 2]	Ein Portbereich, von Port 1 bis Port 2 einschließlich.

Hinweis: Sie können Portlisten und Portbereiche mischen. Beispiel: 80,443,8080-8090

Wenn kein Port angegeben ist, wird der Standardport 80 für `http` und 443 für `https` zugewiesen. Bei der Angabe eines Ports muss das Trennzeichen „:" eingegeben werden.

- **Pfad** (optional)

  Wenn kein Pfad angegeben ist, wird von einem Sternchen (*) ausgegangen, was bedeutet, dass ALLE Pfade zutreffen. Bei der Angabe eines Pfades muss das Trennzeichen „/" eingegeben werden. Es werden keine weiteren Sonderzeichen unterstützt.

Beispiele:

- http://www.juniper.com:80/*
- https://www.juniper.com:443/intranet/*
- *.yahoo.com:80,443/*
- %.danastreet.net:80/share/users/<USER>/*

Angeben von Windows-Dateiressourcen

Kanonisches Format: `\\Server[\Freigabe[\Pfad]]`

Die drei Bestandteile sind:

- **Server** (erforderlich)

  Mögliche Werte:

  - **Hostname**

    Die Systemvariable <USER> kann verwendet werden.

  - **IP-Adresse**

    Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`

  Die beiden vorangehenden umgekehrten Schrägstriche (\\) sind erforderlich.

- **Freigabe** (optional)

  Wenn keine Freigabe angegeben ist, wird von einem Sternchen (*) ausgegangen, was bedeutet, dass ALLE Pfade zutreffen. Die Systemvariable <USER> darf verwendet werden.

- **Pfad** (optional)

  Sonderzeichen sind zulässig, einschließlich:

*****	Entspricht einem beliebigen Zeichen
%	Entspricht einem beliebigen Zeichen außer einem umgekehrten Schrägstrich (\)
?	Entspricht genau einem Zeichen

  Wenn kein Pfad angegeben ist, wird von einem umgekehrten Schrägstrich (\) ausgegangen, d. h., es werden nur die Ordner der obersten Ebene berücksichtigt.

  Beispiele:

  - \\%.danastreet.net\share\<USER>*
  - *.juniper.com\dana*
  - \\10.11.0.10\share\web*
  - \\10.11.254.227\public\%.doc

Angeben von UNIX/NFS-Dateiressourcen

Kanonisches Format: `Server[/Pfad]`

Die beiden Bestandteile sind:

- **Server** (erforderlich)

  Mögliche Werte:

  - **Hostname**

    Die Systemvariable <USER> kann verwendet werden.

  - **IP-Adresse**

    Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`

  Die beiden vorangehenden umgekehrten Schrägstriche (\\) sind erforderlich.

- **Pfad** (optional)

  Sonderzeichen sind zulässig, einschließlich:

*****	Entspricht einem beliebigen Zeichen
%	Entspricht einem beliebigen Zeichen außer einem umgekehrten Schrägstrich (\)
?	Entspricht genau einem Zeichen

  Wenn kein Pfad angegeben ist, wird von einem umgekehrten Schrägstrich (\) ausgegangen, d. h., es werden nur die Ordner der obersten Ebene berücksichtigt.

  Beispiele:

  - %.danastreet.net/share/users/<USER>/*
  - *.juniper.com/dana/*
  - 10.11.0.10/web/*
  - 10.11.254.227/public/%.txt

Angeben von Serverressourcen

Kanonisches Format: `[Protokoll://]Host[:Ports]`

Die drei Bestandteile sind:

- **Protokoll** (optional)

  Hinweis: Nur für Network Connect-Richtlinien verfügbar. Für weitere Ressourcenrichtlinien für Zugriffsfunktionen wie Secure Application Manager oder Telnet/SSH ist die Angabe dieser Bestandteile ungültig.

  Mögliche Werte (Groß- oder Kleinschreibung wird nicht berücksichtigt):

  - tcp
  - udp
  - icmp

  Wenn kein Protokoll angegeben ist, werden alle drei Protokolle angenommen. Bei der Eingabe eines Protokolls muss das Trennzeichen „://" eingegeben werden. Sonderzeichen sind nicht zulässig.

- **Host** (erforderlich)

  Mögliche Werte:

  - **DNS-Hostname**

    Beispiel: www.juniper.com

    Sonderzeichen sind zulässig, einschließlich:

*****	Entspricht ALLEN Zeichen
%	Entspricht einem beliebigen Zeichen außer dem Punkt (.)
?	Entspricht genau einem Zeichen

  - **IP-Adresse/Netzmaske**

    Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`

    Die Netzmaske kann eins der beiden Formate aufweisen:

    - Präfix: Obere Bits
    - IP: `a.b.c.d`

    Beispiel: `10.11.149.2/24` oder `10.11.149.2/255.255.255.0`

    Sonderzeichen sind nicht zulässig.

- **Ports** (optional)

  Mögliche Werte:

*****	Entspricht ALLEN Ports, andere Sonderzeichen sind nicht zulässig.
Port[,Port]*	Eine durch Kommas getrennte Liste einzelner Ports. Gültige Portnummern sind [1-65535].
[Port 1]-[Port 2]	Ein Portbereich, von Port 1 bis Port 2 einschließlich.

Hinweis: Sie können Portlisten und Portbereiche mischen. Beispiel: 80,443,8080-8090

Wenn kein Port angegeben ist, wird der Standardport 80 für `http` und 443 für `https` zugewiesen. Bei der Angabe eines Ports muss das Trennzeichen „:" eingegeben werden.

Beispiele:

- <USER>.danastreet.net:5901-5910
- 10.10.149.149:22,23
- tcp://10.11.0.10:80
- udp://10.11.0.10:*

Angeben von IP-Adresspools

Kanonisches Format: `IP_Bereich`

Der IP-Bereich kann im Format „`a.b.c.d-e`" angegeben werden, wobei der letzte Bestandteil der IP-Adresse ein durch einen Bindestrich (-) begrenzter Bereich ist. Sonderzeichen sind nicht zulässig.

Beispiel:

10.10.10.1-100

Schreiben einer detaillierten Regel

Mit den Zugriffsfunktionen für Web, Dateien, Secure Application Manager, Telnet/SSH und Network Connect können Sie Ressourcenrichtlinien für einzelne Web-, Datei-, Anwendungs- und Telnet-Server angeben. Die Zugriffsfunktionen für Secure Meeting und Email Client verfügen jeweils über eine global anwendbare Richtlinie. Für diese beiden Richtlinien geben Sie Servereinstellungen an, die für alle Rollen verwendet werden, durch die diese Zugriffsfunktionen ermöglicht werden. Für alle anderen Zugriffsfunktionen können Sie eine beliebige Anzahl von Ressourcenrichtlinien angeben und für jede eine oder mehrere detaillierte Regeln definieren.

Eine ***detaillierte Regel*** ist eine Erweiterung einer Ressourcenrichtlinie, die Folgendes angeben kann:

- Zusätzliche[1] Ressourceninformationen (wie bestimmte Pfade, Dateien oder Dateitypen) für Ressourcen, die auf der Registerkarte **General** aufgelistet sind.
- Eine Aktion, die von der auf der Registerkarte **General** angegebenen Aktion abweicht (obwohl die Optionen die gleichen sind).
- Bedingungen, die erfüllt sein müssen, damit die detaillierte Regel angewendet werden kann.

In vielen Fällen ermöglicht die Basis-Ressourcenrichtlinie, d. h. die auf der Registerkarte **General** einer Ressourcenrichtlinie angegebenen Informationen, ausreichende Zugriffssteuerung für eine Ressource:

> Wenn ein Benutzer, der (definierten_Rollen) angehört, versucht, auf (definierte_Ressourcen) zuzugreifen, FÜHRE die angegebene (Ressourcenaktion) AUS.

Sie können eine oder mehrere detaillierte Rollen für eine Richtlinie definieren, wenn Sie eine Aktion durchführen möchten, die auf einer Kombination anderer Informationen basiert, zu denen Folgende gehören können:

- Die Eigenschaften einer Ressource, beispielsweise Header, Inhaltstyp oder Dateityp
- Die Eigenschaften eines Benutzers, beispielsweise der Benutzername und die Rollen, denen er zugeordnet ist

1. Beachten Sie, dass Sie die gleiche Ressourcenliste (wie auf der Registerkarte **General**) auch als detaillierte Regel angeben können, wenn deren einziger Zweck die Anwendung von Bedingungen auf eine Benutzeranforderung ist.

- Die Eigenschaften einer Sitzung, beispielsweise die Quell-IP oder der Browsertyp eines Benutzers, ob der Benutzer die Hostprüfung oder Cachebereinigung ausführt, die Uhrzeit oder Zertifikatattribute

Mit detaillierten Regeln kann die Ressourcenzugriffssteuerung flexibler gestaltet werden, das bestehende Ressourcen- oder Berechtigungsinformationen zum Angeben anderer Anforderungen für andere Benutzer verwendet können, auf die die Basisressourcenrichtlinie angewendet wird.

So schreiben Sie eine detaillierte Regel für eine Ressourcenrichtlinie:

1. Geben Sie auf der Seite **New Policy** für eine Ressourcenrichtlinie die erforderlichen Ressourcen- und Rolleninformationen ein.
2. Wählen Sie im Bereich **Action** die Option **Use Detailed Rules** aus, und klicken Sie auf **Save Changes**.
3. Klicken Sie auf der Registerkarte **Detailed Rules** auf **New Rule**.
4. Führen Sie auf der Seite **Detailed Rule** Folgendes aus:
    1. Konfigurieren Sie im Bereich **Action** die Aktion, die ausgeführt werden soll, wenn die Benutzeranforderung einer Ressource in der Liste **Resource** entspricht (optional). Beachten Sie, dass die auf der Registerkarte **General** angegebene Aktion standardmäßig übertragen wird.
    2. Geben Sie im Bereich **Resources** eine der folgenden Optionen an (erforderlich):
        - Die vollständige oder einen Teil der Ressourcenliste, die auf der Registerkarte **General** angegeben ist.
        - Einen bestimmten Pfad oder eine bestimmte Datei auf den Servern, die auf der Registerkarte **General** angegeben sind. Gegebenenfalls können Platzhalter verwendet werden. Informationen zum Verwenden von Platzhaltern in einer **Resources**-Liste finden Sie in der Dokumentation der entsprechenden Ressourcenrichtlinie.
        - Ein Dateityp, dem gegebenenfalls ein Pfad vorangestellt ist, oder geben Sie einfach `*/*.`*`Dateierweiterung`* an, um Dateien mit der angegebenen Erweiterung innerhalb aller Pfade auf den Servern anzuzeigen, die auf der Registerkarte **General** angegeben sind.
    3. Geben Sie im Abschnitt **Conditions** mindestens einen Ausdruck an, der für die Ausführung der Aktion ausgewertet wird (optional):
        - Boolesche Ausdrücke: Schreiben Sie unter Verwendung von Systemvariablen mindestens einen boolschen Ausdruck mit den Operatoren NOT, OR oder AND. Eine Liste der in Ressourcenrichtlinien verfügbaren Variablen finden Sie unter „Systemvariablen und Beispiele" auf Seite 601.

- Benutzerdefinierte Ausdrücke: Schreiben Sie unter Einhaltung der entsprechenden Syntax mindestens einen benutzerdefinierten Ausdruck. Informationen zur Syntax und zu Variablen finden Sie unter „Schreiben benutzerdefinierter Ausdrücke“ auf Seite 595. Beachten Sie, dass benutzerdefinierte Ausdrücke nur mit der erweiterten Lizenz verfügbar sind.

4 Klicken Sie auf **Save Changes**.

5. Ordnen Sie die Regeln auf der Registerkarte **Detailed Rules** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Sobald das IVE für die vom Benutzer angeforderte Ressource eine entsprechende Ressource in der Liste **Resource** für eine Regel findet, wird die angegebene Aktion durchgeführt und die Verarbeitung der Regeln (und weiterer Ressourcenrichtlinien) beendet.

Benutzerrollen – Übersicht

Eine ***Benutzerrolle*** ist eine Einheit, die die folgenden Einstellungen festlegt: Parameter für Benutzersitzungen (Sitzungseinstellungen und -optionen), individuelle Einstellungen (benutzerdefinierte Einrichtung der Oberfläche und Lesezeichen) und aktivierte Zugriffsfunktionen (Web-, Datei-, Anwendungs-, Netzwerk-, Konferenz- und E-Mail-Zugriff). Eine Benutzerrolle steuert werden den Ressourcenzugriff noch gibt sie andere ressourcenbasierte Optionen für einzelne Anforderungen an. Mithilfe einer Benutzerrolle kann z. B. definiert werden, ob ein Benutzer über die Berechtigung zum Webbrowsing verfügt. Die einzelnen Webressourcen, auf die ein Benutzer zugreifen darf, werden jedoch durch Webressourcen-richtlinien definiert, die separat konfiguriert werden.

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

Informationen zum Erstellen einer Benutzerrolle finden Sie unter „Konfigurieren der Seite „Roles““ auf Seite 393.

Rollenarten

Das IVE unterstützt zwei Arten von Benutzerrollen:

- **Administrators**

  Eine Administratorrolle ist eine Einheit, die die IVE-Verwaltungs-funktionen und -Sitzungseigenschaften für Administratoren angibt, die der Rolle zugeordnet sind. Sie können eine Administratorrolle anpassen, indem Sie Gruppen von IVE-Funktionen und Benutzerrollen auswählen, die Mitglieder der Administratorrolle anzeigen und verwalten dürfen. Weitere Informationen finden Sie unter „Konfigurieren der Seite „Delegation““ auf Seite 355.

- **Users**

  Eine Benutzerrolle ist eine Einheit, die Parameter für Benutzersitzungen, individuelle Einstellungen und aktivierte Zugriffsfunktionen definiert. Sie können eine Benutzerrolle anpassen, indem Sie bestimmte IVE-Zugriffsfunktion aktivieren, Web-, Anwendungs- und Sitzungs-Lesezeichen definieren und Sitzungseinstellungen für die aktivierten Zugriffsfunktionen konfigurieren. Weitere Informationen finden Sie unter „Konfigurieren der Seite „Roles““ auf Seite 393.

Rollenkomponenten

Eine Benutzerrolle enthält die folgenden Informationen:

- **Rolleneinschränkungen** – Die Verfügbarkeit der Rolle für die Benutzer beruht auf den Anforderungen bezüglich Quell-IP, clientseitigem Zertifikat, Hostprüfung und Cachebereinigung, die erfüllt sein müssen, damit ein Benutzer einer Rolle zugewiesen wird.
- **Sitzungsparameter** – Sitzungseinstellungen, u. a. für Höchstdauerwerte (Leerlauf, Maximum, Erinnerung), Warnungen bei Zeitüberschreitung, Roamingsitzungen und Einzelanmeldung sowie Sitzungsoptionen, beispielsweise für permanente Kennwortzwischenspeicherung, beständige Sitzungscookies und Verfolgung der Browseranforderungen.
- **Optionen für die Benutzeroberfläche** – Individuelle Einstellungen, einschließlich Anmeldeseite, Kopf- und Fußzeile der Seiten sowie Anzeige der Browsing-Symbolleiste. Wenn der Benutzer mehreren Rollen zugeordnet ist, zeigt das IVE die Benutzeroberfläche entsprechend der ersten Rolle an, der der Benutzer zugeordnet wurde.
- **Webeinstellungen** – Aktivierung/Deaktivierung der Webzugriffsfunktion, Definition der Weblesezeichen für die Rolle und Optionen für das Webbrowsing. Letzteres kann Folgendes umfassen:
  - Browsingoptionen: User can type URLs, Allow Java applets, Mask hostnames while browsing, Unrewritten pages open in new window
  - Lesezeichenoptionen: User can add bookmarks, Auto-allow role bookmarks
  - Cookieoptionen: Persistent cookies
- **Dateieinstellungen** – Aktivierung/Deaktivierung der Dateizugriffsfunktion, Definition der Dateilesezeichen und Optionen für die Dateinavigation. Letzteres kann Folgendes umfassen:
  - Windows-Netzwerkdateien: User can browse network file shares, User can add bookmarks, Users can add personal bookmarks to Windows folders
  - UNIX-Netzwerkdateien: User can browse network file shares, User can add bookmarks, Users can add personal bookmarks to UNIX/NFS directories

- **Telnet/SSH-Einstellungen** – Aktivierung/Deaktivierung der Zugriffsfunktion Secure Terminal Access, Lesezeichen für Telnet/SSH-Sitzungseinstellungen für diese Rolle und Telnet/SSH-Optionen. Letzteres kann Folgendes umfassen:
  - User can add sessions
  - Auto-allow role Telnet/SSH sessions
- **SAM-Einstellungen** – Aktivierung/Deaktivierung der Zugriffsfunktion Secure Application Manager (J-SAM/W-SAM), Lesezeichen für W-SAM- oder J-SAM-Anwendungen. Letzteres kann Folgendes umfassen:
  - Allgemeine Optionen für Secure Application Manager: Auto-launch Secure Application Manager, Auto-uninstall Secure Application Manager, Auto-allow application servers
  - Optionen für Windows SAM: Auto-upgrade Secure Application Manager
  - Optionen für Java SAM: User can add applications, Automatic host-mapping
- **Einstellungen für Network Connect** – Aktivierung/Deaktivierung der Zugriffsfunktion Network Connect sowie Gewähren von Zugriff auf das lokale Subnetz.
- **Einstellungen für Secure Meeting** – Aktivierung/Deaktivierung der Zugriffsfunktion Secure Meeting und Optionen für Secure Meeting. Dies kann Folgendes umfassen:
  - Allgemeine Optionen: Join and create, authentication requirements, password distribution, remote control
  - Policy settings for number of scheduled meetings, simultaneous meetings, simultaneous meeting attendees, duration of meetings

Konfigurationsanweisungen finden Sie unter „Konfigurieren der Seite „Roles““ auf Seite 393.

Rollenauswertung

Das IVE-Rollenzuordnungsmodul bestimmt die ***Sitzungsrolle*** eines Benutzers bzw. kombinierte Berechtigungen, die für eine Benutzersitzung gültig sind. Dies geschieht wie folgt:

1. Das IVE beginnt die Rollenauswertung mit der ersten Regel auf der Registerkarte **Role Mapping**[1] des Authentifizierungsbereichs, an dem sich der Benutzer erfolgreich anmeldet.
2. Das IVE ermittelt, ob der Benutzer die Bedingungen der Regel erfüllt. Wenn dies der Fall ist, führt das IVE Folgendes durch:

1. Siehe „Rollenzuordnungsregeln“ auf Seite 53.

1. Das IVE fügt die entsprechenden Rollen einer Liste von „zulässigen Rollen" hinzu, zu denen der Benutzer zugeordnet werden kann.
2. Das IVE berücksichtigt dabei, ob konfiguriert wurde, dass die Verarbeitung bei einem Treffer beendet werden soll (Option „Stop on Match"). Wenn dies der Fall ist, fährt das Modul mit Schritt 5 fort.

3. Gemäß Prozessschritt 2 wertet das IVE die nächste Regel aus, die auf der Registerkarte **Role Mapping** des Authentifizierungsbereichs angegeben ist. Dies wird für alle folgenden Regeln wiederholt, bis alle Rollenzuordnungsregeln ausgewertet sind und das IVE eine vollständige Liste der zulässigen Rollen aufgestellt hat.
4. Das IVE wertet die Definitionen aller Rollen in der Liste der zulässigen Rollen aus und überprüft, ob der Benutzer Rolleneinschränkungen unterliegt. Das IVE erstellt anhand dieser Informationen eine Liste der ***gültigen Rollen***, d. h. der Rollen, für die der Benutzer zusätzliche Anforderungen erfüllt.

   Wenn die Liste gültiger Rollen nur eine Rolle enthält, ordnet das IVE den Benutzer dieser Rolle zu. Andernfalls setzt das IVE die Auswertung fort.
5. Für Benutzer, die mehreren Rollen zugeordnet sind, wertet das IVE die Einstellung aus, die auf der Registerkarte **Role Mapping** angegeben ist.
   - **Merge settings for all assigned roles**

     Wenn Sie diese Option auswählen, führt das IVE eine permissive Zusammenführung aller gültigen Benutzerrollen durch, um die Gesamtrolle (Netzrolle) für eine Benutzersitzung zu ermitteln.
   - **User must select from among assigned roles**

     Wenn Sie diese Option auswählen, gibt das IVE einem authentifizierten Benutzer eine Liste zulässiger Rollen aus. Der Benutzer muss eine Rolle aus der Liste auswählen, und das IVE weist den Benutzer dann für die Dauer der Benutzersitzung dieser Rolle zu.

Richtlinien für permissive Zusammenführungen

Eine ***permissive Zusammenführung*** ist eine Zusammenführung, die *aktivierte* Funktionen und Einstellungen anhand der folgenden Richtlinien kombiniert.

- Die Aktivierung einer Zugriffsfunktion in einer Rolle hat Vorrang vor der Deaktivierung der gleichen Funktion in einer anderen Rolle. Wenn beispielsweise Secure Meeting für eine Rolle, der ein Benutzer angehört, deaktiviert, für eine andere Rolle jedoch aktiviert ist, darf der Benutzer Secure Meeting in dieser Benutzersitzung verwenden.
- Bei Secure Application Manager aktiviert das IVE die Version, die der ersten Rolle entspricht, für die diese Funktion aktiviert ist. Außerdem führt das IVE die Einstellungen aller Rollen zusammen, die der ausgewählten Version entsprechen.

- Bei den Optionen für die Benutzeroberfläche wendet das IVE die Einstellungen an, die der ersten Rolle entsprechen, der der Benutzer zugeordnet ist.
- Bei Überschreitungen der Sitzungsdauer wendet das IVE den höchsten Wert aller Rollen auf die Benutzersitzung an.
- Wenn die Roaming-Sitzungsfunktion für mehrere Rollen aktiviert ist, führt das IVE die Netzmasken zusammen, um die Netzmaske für die Sitzung zu erweitern.

Teil 2
IVE-Funktionen

In diesem Abschnitt werden die Funktionen des Access Series-Produkts beschrieben. Für einige dieser Funktionen sind weitere Lizenzen erforderlich.

Inhalt

Cachebereinigung – Übersicht

Bei der Cachebereinigung handelt es sich um einen Client-Agent, der übrig gebliebene Daten wie temporäre Dateien oder Anwendungscaches nach einer IVE-Sitzung vom Benutzercomputer entfernt. Wenn sich beispielsweise ein Benutzer von einem Internet-Kiosk beim IVE anmeldet und mithilfe eines Browser-Plug-Ins ein Microsoft Word-Dokument öffnet, entfernt die Cachebereinigung nach Beenden der Sitzung die im Browsercache (im Ordner „Windows") gespeicherte temporäre Kopie der Word-Datei. Durch das Entfernen der Kopie verhindert die Cachebereinigung, dass andere Benutzer des Kiosks das Word-Dokument suchen und öffnen können, nachdem der IVE-Benutzer seine Sitzung beendet hat. Sie können auch festlegen, dass durch die Cachebereinigung Inhalte sowie bestimmte Dateien und Ordner spezifischer Hosts und Domänen gelöscht werden.

Sie können den Zugriff auf das IVE und die Ressourcen durch die Cachebereinigung einschränken:

- **Richtlinie für Bereichsauthentifizierung**

  Wenn Administratoren versuchen, sich beim IVE anzumelden, wertet das IVE die Authentifizierungsrichtlinie des angegebenen Bereichs aus und ermittelt, ob die Cachebereinigung zu den Anforderungen gehört, die vor der Authentifizierung erfüllt sein müssen. Sie können eine Richtlinie für die Bereichsauthentifizierung so konfigurieren, dass die Cachebereinigung heruntergeladen wird, die Cachebereinigung heruntergeladen und ausgeführt wird oder dass die Cachebereinigung nicht erforderlich ist. Der Benutzer muss sich von einem Computer anmelden, der den Cachebereinigung-Anforderungen entspricht, die für den Bereich festgelegt wurden. Wenn dies nicht der Fall ist, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und der Benutzer kann nicht auf das IVE zugreifen.

- **Benutzerrolle**

  Wenn das IVE die Liste der geeigneten Rollen ermittelt, denen ein Administrator oder Benutzer zugeordnet ist, wertet es die Einschränkungen der einzelnen Rollen aus, um zu ermitteln, ob die Rolle die Ausführung der Cachebereinigung auf der Arbeitsstation des Benutzers erfordert. Wenn dies der Fall ist und das Gerät des Benutzers die Cachebereinigung noch nicht ausführt, ordnet das IVE den Benutzer dieser Rolle nicht zu.

- **Ressourcenrichtlinie**

  Wenn ein Benutzer eine Ressource anfordert, wertet das IVE die detaillierten Regeln der Ressourcenrichtlinie aus, um zu ermitteln, ob die Cachebereinigung auf der Arbeitsstation des Benutzers installiert werden muss oder bereits ausgeführt wird. Das IVE verweigert den Zugriff auf die betreffende Ressource, wenn das Gerät des Benutzers nicht der festgelegten Cachebereinigung-Richtlinie entspricht.

Ausführen der Cachebereinigung

Wenn Sie die Cachebereinigung als Anforderung für eine Rolle oder Ressourcenrichtlinie festlegen möchten, muss der Agent bei der Anmeldung des Benutzers minimal installiert werden. Dies wird in der Authentifizierungsrichtlinie des Bereichs konfiguriert. Bei dieser Konfiguration lädt das IVE das ActiveX-Steuerelement auf das Benutzersystem herunter. Die Cachebereinigung wird in dem Intervall ausgeführt, das Sie auf der Registerkarte **System > Configuration > Security > Cache Cleaner** konfigurieren[1]. Für die Ausführung der Cachebereinigung muss auf den Benutzercomputern ActiveX aktiviert sein.

Hinweis: ActiveX-Steuerelemente werden für Administratoren und Hauptbenutzer in Windows 2000-Systemen automatisch aktiviert, Standardbenutzer müssen sie hingegen manuell aktivieren. Um ActiveX-Steuerelemente in Internet Explorer zu aktivieren, wählen Sie **Extras > Internetoptionen > Sicherheit > Anpassen** aus, und aktivieren Sie anschließend im Dialogfeld **Sicherheitseinstellungen** die ActiveX-Komponenten.

Cachebereinigung führt in folgenden Situationen eine endgültige Bereinigung aus:

- **Der Benutzer meldet sich explizit von seiner Benutzersitzung ab**

  Wenn ein Benutzer auf der IVE-Startseite auf **Sign Out** klickt, führt die Cachebereinigung eine endgültige Bereinigung aus und deinstalliert sich anschließend selbst vom Benutzersystem.

- **Die Höchstdauer für die Benutzersitzung ist überschritten**

  Wenn eine Zeitüberschreitung einer Benutzersitzung auftritt, führt die Cachebereinigung eine Bereinigung durch. Wenn sich der Benutzer erneut anmeldet, führt die Cachebereinigung eine erneute Bereinigung durch. Die Cachebereinigung überprüft in bestimmten Abständen die Gültigkeit einer Sitzung und erkennt daher, wann eine Sitzungszeitüberschreitung auftritt. Die entsprechenden Intervalle werden auf der Registerkarte **System > Configuration > Security > Cache Cleaner** angegeben (siehe „Registerkarte „Security > Cache Cleaner““ auf Seite 174).

  Hinweis: Bei der Überprüfung der Gültigkeit einer Sitzung stellt die Cachebereinigung eine Verbindung mit dem IVE her. Durch diese Aktion können an persönlichen Firewalls Warnmeldungen ausgegeben werden. Benutzer müssen diesen Datenverkehr zulassen, damit die Cachebereinigung ordnungsgemäß ausgeführt werden kann.

1. Benutzern mit einer persönlichen Firewall wird beim Leeren des Cache durch die Cachebereinigung ein Protokolleintrag angezeigt.

- **Ein Clientsystem wird nach einem nicht ordnungsgemäßen Herunterfahren des Systems bzw. einem nicht ordnungsgemäßen Abbruch der Sitzung oder der Verbindung neu gestartet.**

  Die Cachebereinigung führt eine endgültige Bereinigung aus und deinstalliert sich nach dem Neustart des Systems selbst vom Benutzersystem.

Die Cachebereinigung protokolliert keine Einträge im IVE-Standardprotokoll, sondern in einer temporären Client-Textdatei.

```
c:\Program Files\Neoteris\Cache Cleaner\dsCacheCleaner.log
```

Dieses verschlüsselte Protokoll wird gelöscht, wenn sich die Cachebereinigung selbst deinstalliert. Sie können die clientseitige Protokollierung auf der Registerkarte **System > Configuration > Security > Client-side Logs** deaktivieren.

Wichtig: Die Cachebereinigung bereinigt bzw. löscht weder den Browserverlauf noch vom Benutzer explizit gespeicherten Dateien, Internet Explorer-Plug-Ins, ActiveX-Steuerelemente oder Einträge in `index.dat` (eine private Tabelle von URLs, die von Internet Explorer verwaltet wird).

Weitere Informationen zu den Optionen der Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 25.

Central Manager – Übersicht

Central Manager ist ein zweischichtiges System (Client/Server) für die Verwaltung mehrerer IVEs, unabhängig davon, ob diese sich in einem Cluster befinden. Central Manager enthält Folgendes:

- **System-Dashboard**

  Die Dashboard-Funktion von Central Manager zeigt Diagramme und Warnhinweise zur Systemkapazität an und ermöglicht Ihnen damit die komfortable Überwachung des Systems. (Seite 147)

- **Verbesserte Protokollierung und Überwachung**

  Sie können eigene Filter für die Protokollierung erstellen, sodass Sie nur ausgewählte Protokollmeldungen im gewünschten Format anzeigen und speichern können. (Seite 249)

- **Konfigurationsübertragung**

  Die Funktion für die Konfigurationsübertragung ermöglicht eine komfortable, zentrale Verwaltung, da Sie Einstellungen ganz einfach von einem IVE auf ein anderes übertragen können. (Seite 538)

- **Ausfallfreie Aktualisierung**

  Die Funktion für ausfallfreie Aktualisierung beschleunigt die Aktualisierung innerhalb eines Clusters, da sie gewährleistet, dass ein Clustermitglied während des Vorgangs immer funktionstüchtig ist. (Seite 525)

- **Verbesserte Benutzeroberfläche**

  Die Oberfläche der Webkonsole für Central Manager wurde ansprechender gestaltet.

Zertifikate – Übersicht

Das IVE sichert die über das Internet an Clients gesendeten Daten mithilfe der PKI. ***PKI*** (Public Key Infrastructure) ist eine Sicherheitsmethode, bei der öffentliche und private Schlüssel zum Verschlüsseln und Entschlüsseln von Informationen verwendet werden. Diese Schlüssel werden über digitale Zertifikate aktiviert und gespeichert. Ein ***digitales Zertifikat*** ist eine verschlüsselte elektronische Datei, in der die Anmeldeinformationen eines Webservers oder Benutzers für Client-Server-Transaktionen festgelegt werden. Das IVE verwendet folgende Typen digitaler Zertifikate zum Festlegen von Anmeldeinformationen und zum Sichern von IVE-Transaktionen:

- **Serverzertifikate**

  Durch ein ***Serverzertifikat*** wird der Netzwerkverkehr zum und vom IVE mithilfe bestimmter Elemente gesichert. Dies umfasst beispielsweise den Firmennamen, eine Kopie des öffentlichen Schlüssels Ihres Unternehmens, die digitale Signatur der Zertifizierungsstelle (Certificate Authority, CA), die das Zertifikat ausgestellt hat, eine Seriennummer sowie ein Ablaufdatum.

  Wenn der Clientbrowser verschlüsselte Daten vom IVE empfängt, überprüft er zuerst, ob das Zertifikat des IVE gültig ist und ob der Benutzer der Zertifizierungsstelle vertraut, die das Zertifikat des IVE ausgestellt hat. Sofern der Benutzer nicht bereits angegeben hat, dass er dem IVE-Zertifikataussteller vertraut, wird er vom Webbrowser aufgefordert, das Zertifikat des IVE zu akzeptieren oder zu installieren.

  Beim Initialisieren des IVE wird lokal ein temporäres, selbst signiertes digitales Zertifikat erstellt, mit dem die Benutzer sofort Ihr IVE[1] verwenden können. Wenn Sie das selbst signierte Zertifikat des IVE jedoch nicht verwenden möchten, können Sie eine digitale Serverzertifikatdatei und den zugehörigen privaten Schlüssel in das IVE importieren. Weitere Informationen finden Sie unter „Registerkarte „Certificates > Server Certificates““ auf Seite 179. Wenn Sie über eine erweiterte Lizenz verfügen, können Sie mehrere Serverzertifikate in das IVE importieren. Weitere Informationen finden Sie unter „Mehrere Serverzertifikate" auf Seite 71.

1. Die Verschlüsselung für das während der Initialisierung erstellte selbst signierte Zertifikat ist zwar absolut sicher, für die Benutzer wird jedoch trotzdem bei jeder Anmeldung beim IVE eine Sicherheitswarnung angezeigt, da das Zertifikat nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wird. Zu Produktionszwecken empfiehlt es sich, ein digitales Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle anzufordern.

- **Appletzertifikate**

  Bei einem ***Appletzertifikat*** (oder Codesignaturzertifikat) handelt es sich um ein serverseitiges Zertifikat, das die vom IVE vermittelten Java-Applets neu signiert. Sie haben entweder die Möglichkeit, das auf dem IVE vorinstallierte selbst signierte Appletzertifikat zu verwenden oder ein eigenes Codesignaturzertifikat zu installieren. Weitere Informationen finden Sie unter „Appletzertifikate" auf Seite 72.

Für eine IVE-Basisinstallation sind nur diese Zertifikate erforderlich. Das IVE kann alle Java-Applets mit einem einzigen Appletzertifikat neu signieren und alle weiteren PKI-basierten Interaktionen mit einem einzigen Serverzertifikat vermitteln.

Sollten diese Basiszertifikate jedoch nicht Ihren Anforderungen entsprechen, können Sie mehrere Server- und Appletzertifikate auf dem IVE installieren oder Zertifizierungsstellenzertifikate verwenden, um Benutzer zu überprüfen. Mit einem ***Zertifizierungsstellenzertifikat*** können Sie den Zugriff auf Bereiche, Rollen und Ressourcenrichtlinien auf der Grundlage von Zertifikaten oder Zertifikatattributen steuern. So können Sie beispielsweise festlegen, dass Benutzer ein gültiges clientseitiges Zertifikat mit dem auf „eigenefirma.com" festgelegten Organisationseinheitsattribut vorlegen müssen, um sich am Authentifizierungsbereich „Users" anmelden zu können. Weitere Informationen zu Zertifikatüberprüfungen von Bereichen, Rollen und Ressourcenrichtlinien finden Sie unter „Zertifikateinschränkungen" auf Seite 587.

Damit Sie Zertifizierungsstellenzertifikate verwenden können, müssen Sie die richtigen Zertifikate auf dem IVE installieren und aktivieren sowie die entsprechenden clientseitigen Zertifikate für die Webbrowser der Endbenutzer installieren. Beim Überprüfen der Benutzer mit Zertifizierungsstellenzertifikaten prüft das IVE, ob das Zertifikat abgelaufen oder beschädigt ist und ob es von einer vom IVE anerkannten Zertifizierungsstelle signiert wurde. Im Falle eines verketteten Zertifizierungsstellenzertifikats (siehe unten) verfolgt das IVE außerdem die Kette der Zertifikataussteller bis zur Stammzertifizierungsstelle zurück, wobei die Gültigkeit jedes einzelnen Ausstellers überprüft wird. Weitere Informationen finden Sie unter „Registerkarte „Certificates > CA Certificates"" auf Seite 190.

Das IVE unterstützt die Verwendung folgender zusätzlicher Features für Zertifizierungsstellenzertifikate:

- **Zertifikatserver**

  Ein ***Zertifikatserver*** ermöglicht es Ihnen, IVE-Benutzer lediglich auf Grundlage der zugehörigen Zertifikatattribute zu authentifizieren, statt sie über einen Standardauthentifizierungsserver (wie LDAP oder SiteMinder) zu authentifizieren und bestimmte Zertifikate oder Zertifikatattribute anzufordern. Weitere Informationen finden Sie unter „Konfigurieren einer Zertifikatserverinstanz" auf Seite 299.

- **Zertifikathierarchien**

  Innerhalb einer ***Zertifikathierarchie*** sind untergeordnete Zertifikate, die auch als Zwischenzertifikate bezeichnet werden, einem Stammzertifikat untergeordnet. Jedes ***Zwischenzertifikat*** (auch als verkettetes Zertifikat bezeichnet) verarbeitet Anforderungen für einen Teil der Domäne der Stammzertifizierungsstelle. Sie können beispielsweise ein Stammzertifikat erstellen, das sämtliche Anforderungen an die Domäne **eigenefirma.com** verarbeitet, und diesem anschließend Zwischenzertifikate unterordnen, die Anforderungen an **partner.eigenefirma.com** und **mitarbeiter.eigenefirma.com** verarbeiten. Darüber hinaus können Sie auch Vertrauensstellungen zwischen verschiedenen Zertifikathierarchien herstellen. Weitere Informationen finden Sie unter „Zertifikathierarchien" auf Seite 74.

- **Zertifikatsperrlisten**

  Bei der ***Zertifikatssperrung*** handelt es sich um einen Mechanismus, bei dem eine Zertifizierungsstelle die Gültigkeit eines Zertifikats vor dem Ablaufdatum aufhebt. Eine ***Zertifikatsperrliste (Certificate Revocation List, CRL)*** ist eine von einer Zertifizierungsstelle veröffentlichte Liste gesperrter Zertifikate. In Zertifikatsperrlisten enthält jeder Eintrag die Seriennummer des gesperrten Zertifikats, das Datum sowie den Grund der Zertifikatssperrung. Die Zertifizierungsstelle kann die Gültigkeit eines Zertifikats aus vielen verschiedenen Gründen aufheben, z. B. wenn ein Mitarbeiter, für den das Zertifikat ausgestellt wurde, das Unternehmen verlassen hat, der private Schlüssel des Zertifikats gefährdet ist oder das clientseitige Zertifikat verloren gegangen ist oder gestohlen wurde. Nachdem die Zertifizierungsstelle ein Zertifikat gesperrt hat, kann das IVE Benutzern, die ein gesperrtes Zertifikat vorlegen, den Zugriff entsprechend verweigern. Weitere Informationen finden Sie unter „Zertifikatsperrlisten" auf Seite 75.

Mehrere Serverzertifikate

Bei Verwendung mehrerer Serverzertifikate prüft jedes Zertifikat die Gültigkeit für einen separaten Hostnamen oder für einen vollständig qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN), wobei jedes Zertifikat von einer anderen Zertifizierungsstelle ausgestellt werden kann. Sie können mehrere Stammzertifikate zusammen mit mehreren Anmelde-URLs verwenden. Mit der Funktion für mehrere Anmelde-URLs können Sie den Zugriff auf das IVE für mehrere Hostnamen bereitstellen, indem Sie für jeden Hostnamen oder FQDN einen anderen Anmelde-URL erstellen. Anschließend können Sie separate Anmeldeseiten und Authentifizierungsanforderungen für jeden Anmelde-URL erstellen (Seite 267). Dank der Funktion für mehrere Serverzertifikate haben Sie die Möglichkeit, verschiedene Zertifikate zu verwenden, um Benutzer zu überprüfen, die sich über jeden dieser Hostnamen oder FQDN anmelden. So können Sie beispielsweise ein Zertifikat der Site `partner.eigenefirma.com` und ein anderes Zertifikat der Site `mitarbeiter.eigenefirma.com` zuordnen.

Zum Aktivieren mehrerer Serverzertifikate gehen Sie folgendermaßen vor:

1. Geben Sie die IP-Adressen an, über die die Benutzer möglicherweise auf das IVE zugreifen, und erstellen Sie dann für jede IP-Adresse einen virtuellen Port. Ein ***virtueller Port*** aktiviert einen IP-Alias für einen physischen Port. So erstellen Sie virtuelle Ports für interne und externe Benutzer:
   - **Interne Benutzer**

     Verwenden Sie die Einstellungen auf der Registerkarte **System > Network > Internal Port > Virtual Port**, um virtuelle Ports für Benutzer (z. B. Mitarbeiter) zu erstellen, die sich innerhalb des internen Netzwerks beim IVE anmelden (Seite 212).
   - **Externe Benutzer**

     Verwenden Sie die Einstellungen auf der Registerkarte **System > Network > External Port > Virtual Port**, um virtuelle Ports für Benutzer (z. B. Kunden und Partner) zu erstellen, die sich außerhalb Ihres internen Netzwerks beim IVE anmelden (Seite 219).
2. Laden Sie die Serverzertifikate auf das IVE hoch. Sie können Zertifikate von der Seite **System > Configuration > Certificates** > **Server Certificates** der Webkonsole (Seite 179) oder von der Seite **Maintenance > Import/Export > System Configuration** der Webkonsole importieren (Seite 530). Laden Sie jeweils ein Serverzertifikat für jede Domäne (Hostname) hoch, die Sie auf dem IVE hosten möchten.
3. Geben Sie mithilfe der Einstellungen auf der Registerkarte **System > Configuration > Certificates > Server Certificates** an, welche virtuellen Ports das IVE den Zertifikaten zuordnen soll. Wenn ein Benutzer versucht, sich mit der für einen virtuellen Port definierten IP-Adresse beim IVE anzumelden, verwendet das IVE das dem virtuellen Port zugeordnete Zertifikat, um die SSL-Transaktion zu initiieren (Seite 212).

Appletzertifikate

Wenn das IVE ein signiertes Java-Applet vermittelt, signiert es das Applet mit einem selbst signierten Zertifikat neu, das von einer nicht standardmäßig vertrauenswürdigen Stammzertifizierungsstelle ausgestellt wurde. Wenn ein Benutzer ein Applet anfordert, das Aufgaben mit einem hohen Risikopotential durchführt, z. B. Zugreifen auf Netzwerkserver, wird im Browser des Benutzers in einer Sicherheitswarnung angezeigt, dass der Stamm nicht vertrauenswürdig ist. Um die Anzeige dieser Warnung zu vermeiden, können Sie ein Codesignaturzertifikat importieren, mit dem das IVE zu vermittelnde Applets neu signiert.

Folgende Codesignaturzertifikate werden unterstützt:

- **Microsoft Authenticode-Zertifikat**

  Mit diesem Zertifikat signiert das IVE Applets, die über MS JVM oder SUN JVM ausgeführt werden. Beachten Sie, dass nur von Verisign ausgestellte Microsoft Authenticode-Zertifikate unterstützt werden.

- **JavaSoft-Zertifikat**

  Mit diesem Zertifikat signiert das IVE Applets, die über SUN JVM ausgeführt werden. Beachten Sie, dass nur von Verisign und Thawte ausgestellte JavaSoft-Zertifikate unterstützt werden.

Beachten Sie bei der Auswahl des zu importierenden Codesignaturzertifikats folgende Browserabhängigkeiten:

- **Internet Explorer**

  Auf neuen Computern, auf denen bei der Lieferung Windows XP vorinstalliert ist, wird in Internet Explorer normalerweise die SUN JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit dem JavaSoft-Zertifikat neu signiert werden müssen.

  Auf PCs unter Windows 98 oder 2000 oder auf PCs, die auf Windows XP aktualisiert wurden, wird in Internet Explorer normalerweise MS JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit einem Authenticode-Zertifikat neu signiert werden müssen.

- **Netscape**

  Netscape-Browser unterstützen nur die SUN JVM. Dies bedeutet, dass Applets vom IVE mit dem JavaSoft-Zertifikat neu signiert werden müssen.

Weitere Hinweise für Benutzer der SUN JVM:

- Standardmäßig werden Applets vom Java-Plug-In zusammen mit dem Codesignaturzertifikat zwischengespeichert, das beim Benutzerzugriff auf das Applet bereitgestellt wird. Der Browser stellt Applets also auch nach dem Importieren eines Codesignaturzertifikats in das IVE weiterhin mit dem ursprünglichen Zertifikat bereit. Um sicherzustellen, dass Benutzer der SUN JVM keine Aufforderungen für nicht vertrauenswürdige Zertifikate für Applets erhalten, auf die sie vor dem Import eines Codesignaturzertifikats zugegriffen haben, muss der Cache des Java-Plug-Ins geleert werden. Alternativ können Benutzer den Cache deaktivieren. Durch diese Option kann jedoch die Leistung beeinträchtigt werden, da das Applet bei jedem Benutzerzugriff abgerufen werden muss.

- Das Java-Plug-In verwaltet eine eigene Liste vertrauenswürdiger Webserverzertifikate, die sich von der entsprechenden Liste des Browsers unterscheidet. Wenn ein Benutzer auf ein Applet zugreift, stellt die SUN JVM (zusätzlich zum Browser) eine eigene Verbindung mit dem Webserver her, auf dem sich das Applet befindet. Dem Benutzer wird daraufhin die Option zur Verfügung gestellt, zusätzlich zum Codesignaturzertifikat das Webserverzertifikat anzunehmen. In solchen Fällen muss der Benutzer die Schaltfläche Always Trust für das Webserverzertifikat auswählen. Aufgrund einer integrierten Zeitüberschreitung im Java-Plug-In wird das Applet nicht geladen, wenn der Benutzer bei der Auswahl dieser Schaltfläche für das Webserverzertifikat zu lange wartet.

Zertifikathierarchien

Innerhalb einer Zertifikathierarchie sind Zwischenzertifikate einem einzigen Stammzertifikat untergeordnet. Das Stammzertifikat wird von einer Stammzertifizierungsstelle ausgestellt, ist selbst signiert und fungiert als Masterzertifizierungsstelle für die gesamte Domäne. Jedes Zwischenzertifikat wird von einer Zwischenzertifizierungsstelle signiert, vom übergeordneten Zertifikat in der Kette als vertrauenswürdig angesehen und überprüft Benutzer in einem Unterabschnitt der Domäne.

Zum Aktivieren der Authentifizierung in einer Umgebung mit verketteten Zertifikaten müssen Sie die jeweiligen clientseitigen Zertifikate für jeden Webbrowser der Benutzer installieren und anschließend die entsprechenden Zertifizierungsstellenzertifikate über die Seite **System > Configuration > Certificates > CA Certificates** der Webkonsole[1] auf das IVE hochladen. Sie müssen zum Hochladen der Zertifikatkette auf das IVE eine der folgenden Methoden anwenden:

- **Importieren der gesamten Zertifikatkette**

  Beim Installieren einer Kette von Zertifikaten einer einzigen Datei importiert das IVE das Stammzertifikat sowie alle untergeordneten Zertifikate, deren übergeordnete Zertifikate sich in der Datei oder auf dem IVE befinden. Sie können die Zertifikate in einer beliebigen Reihenfolge in die Importdatei einschließen.
- **Importieren einzelner Zertifikate in absteigender Reihenfolge**

  Beim Installieren einer Kette von Zertifikaten aus mehreren Dateien setzt das IVE voraus, dass Sie zuerst das Stammzertifikat und danach die restlichen verketteten Zertifikate in absteigender Reihenfolge installieren.

1. Mit einer Basislizenz sind Sie nicht in der Lage, eine Kette zu installieren, deren Zertifikate von unterschiedlichen Zertifizierungsstellen ausgestellt werden. Die Zertifizierungsstelle, die das Zertifikat der untersten Ebene in der Kette signiert, muss auch alle anderen Zertifikate in der Kette (mit Ausnahme des selbst signierten Stammzertifikats) signieren.

Wenn Sie verkettete Zertifikate mithilfe einer dieser Methoden installieren, verkettet das IVE die Zertifikate automatisch in der richtigen Reihenfolge und zeigt sie hierarchisch in der Webkonsole an.

Hinweis: Wenn Sie mehrere Zertifikate für den Webbrowser eines Benutzers installieren, wird der Benutzer vom Browser aufgefordert, das bei jeder Anmeldung beim IVE zu verwendende Zertifikat auswählen.

Anweisungen hierfür finden Sie unter „Registerkarte „Certificates > CA Certificates““ auf Seite 190.

Zertifikatsperrlisten

Eine ***Zertifikatsperrliste (Certificate Revocation List, CRL)*** dient als Mechanismus für das Stornieren eines clientseitigen Zertifikats. Wie bereits aus dem Namen hervorgeht, handelt es sich bei einer Zertifikatsperrliste um eine von einer Zertifizierungsstelle oder von einem delegierten CRL-Aussteller veröffentlichte Liste gesperrter Zertifikate. Das IVE unterstützt ***Basis-CRLs***, die alle gesperrten Zertifikate des Unternehmens in einer vereinheitlichten Liste enthalten.

Das IVE erkennt die zu verwendende Zertifikatsperrliste anhand der Überprüfung des Clientzertifikats. (Beim Ausstellen eines Zertifikats schließt die Zertifizierungsstelle CRL-Informationen für das Zertifikat im Zertifikat selbst ein.) Damit sichergestellt ist, dass das IVE die aktuellsten CRL-Informationen erhält, kommuniziert es regelmäßig mit einem Sperrlisten-Verteilungspunkt, um eine aktualisierte Liste der gesperrten Zertifikate abzurufen. Bei einem ***Sperrlisten-Verteilungspunkt*** handelt es sich um einen Speicherort auf einem LDAP-Verzeichnisserver oder auf einem Webserver, der von einer Zertifizierungsstelle zum Veröffentlichen von Zertifikatsperrlisten verwendet wird. Das IVE lädt die Zertifikatsperrliste vom Sperrlisten-Verteilungspunkt herunter, und zwar in dem in der CRL angegebenen Intervall, in dem von Ihnen während der CRL-Konfiguration angegebenen Intervall und wenn Sie die Zertifikatsperrliste manuell herunterladen.

Zertifizierungsstellen schließen zwar CRL-Informationen in clientseitigen Zertifikaten ein, die Daten für Sperrlisten-Verteilungspunkte werden jedoch nicht immer berücksichtigt. Eine Zertifizierungsstelle hat folgende Möglichkeiten, um das IVE über den Ort des Sperrlisten-Verteilungspunkts eines Zertifikats zu informieren:

- **Angeben der Sperrlisten-Verteilungspunkte im Zertifizierungsstellenzertifikat**

  Wenn die Zertifizierungsstelle ein Zertifizierungsstellenzertifikat ausstellt, kann sie dabei ein Attribut hinzufügen, das den Ort des Sperrlisten-Verteilungspunktes angibt, auf den das IVE zugreifen soll. Wenn mehrere Sperrlisten-Verteilungspunkte angegeben sind, wählt das IVE den ersten im Zertifikat aufgelisteten Punkt und wechselt dann ggf. zu den nachfolgenden Sperrlisten-Verteilungspunkten.

- **Angeben der Sperrlisten-Verteilungspunkte in Clientzertifikaten**

  Wenn die Zertifizierungsstelle clientseitige Zertifikate ausstellt, kann sie dabei ein Attribut hinzufügen, das den Ort des Sperrlisten-Verteilungspunktes angibt, auf den das IVE zugreifen soll. Wenn mehrere Sperrlisten-Verteilungspunkte angegeben sind, wählt das IVE den ersten im Zertifikat aufgelisteten Punkt und wechselt dann ggf. zu den nachfolgenden Sperrlisten-Verteilungspunkten.

  Hinweis: Wenn Sie sich diese Methode auswählen, erhält der Benutzer bei der ersten Anmeldung beim IVE eine Fehlermeldung, weil keine CRL-Informationen verfügbar sind. Nachdem das IVE das Clientzertifikat erkannt und den CRL-Ort extrahiert hat, kann es mit dem Herunterladen der Zertifikatsperrliste beginnen und anschließend das Zertifikat des Benutzers überprüfen. Zwecks erfolgreicher Anmeldung beim IVE muss der Benutzer nach ein paar Sekunden erneut versuchen, die Verbindung herzustellen.

- **Auffordern des Administrators zur manuellen Eingabe des Orts des Sperrlisten-Verteilungspunktes**

  Wenn die Zertifizierungsstelle keinen Ort des Sperrlisten-Verteilungspunktes in den Client- oder Zertifizierungsstellenzertifikaten angegeben hat, müssen Sie beim Konfigurieren des IVE manuell festlegen, wie das gesamte CRL-Objekt heruntergeladen werden soll. Sie können einen primären und einen Sicherungs-Sperrlisten-Verteilungspunkt angeben. (Die manuelle Eingabe des Orts des Sperrlisten-Verteilungspunktes bietet Ihnen die größte Flexibilität, da Sie die Zertifikate nicht neu ausstellen müssen, wenn Sie den Ort des Sperrlisten-Verteilungspunktes ändern.)

Das IVE überprüft das Zertifikat des Benutzers während der Authentifizierung anhand der entsprechenden Zertifikatsperrliste. Wenn das IVE ermittelt, dass das Zertifikat des Benutzers gültig ist, werden die Zertifikatattribute zwischengespeichert und ggf. bei den Überprüfungen der Rollen und Ressourcenrichtlinien angewendet. Wenn das IVE ermittelt, dass das Zertifikat des Benutzers ungültig ist, wenn es nicht die entsprechende Zertifikatsperrliste abrufen kann oder die Zertifikatsperrliste abgelaufen ist, wird dem Benutzer der Zugriff verweigert.

Wichtig:

- Das IVE unterstützt nur Zertifikatsperrlisten im PEM- oder DER-Format, die von der Zertifizierungsstelle signiert wurden, für die diese Sperrungen gelten.
- Das IVE speichert nur die erste Zertifikatsperrliste in einer PEM-Datei.
- Das IVE bietet keine Unterstützung für die IDP-Erweiterung (Issuing Distribution Point) für Zertifikatsperrlisten.

Konfigurationsanweisungen finden Sie unter „Aktivieren der CRL-Prüfung" auf Seite 194.

Cluster – Übersicht

Sie können eine Clusterlizenz für die Bereitstellung von zwei bis acht Secure Access Series- oder Secure Access Series FIPS-Appliances als Cluster erwerben. Die IVE-Plattform unterstützt in einem LAN oder WAN Aktiv/Passiv- oder Aktiv/Aktiv-Konfigurationen, um hohe Verfügbarkeit, verbesserte Skalierbarkeit und Lastenausgleich zu gewährleisten.

In diesem Abschnitt erhalten Sie eine Übersicht über Cluster. Informationen zur Vorgehensweise finden Sie unter:

Cluster – Übersicht

Sie legen einen Cluster in einem IVE mithilfe der folgenden drei Angaben fest:

1. Eine Bezeichnung für den Cluster
2. Ein gemeinsames Kennwort für die Clustermitglieder
3. Einen Namen, der das IVE im Cluster kennzeichnet

Nachdem Sie diese Daten auf der Registerkarte **System > Clustering > Create** angegeben haben, klicken Sie auf **Create Cluster**, um den Cluster zu initiieren und das aktuelle IVE zum Cluster hinzuzufügen. Nach dem Erstellen des Clusters werden auf der Seite **Clustering** die Registerkarten **Status** und **Properties** angezeigt, durch die die ursprünglichen Registerkarten **Join** und **Create** ersetzt werden. Die Registerkarte **Status** enthält den Clusternamen und –typ sowie die Konfiguration (aktiv/aktiv bzw. aktiv/passiv). Auf dieser Registerkarte können Sie neue Mitglieder angeben sowie bestehende Mitglieder verwalten, und es werden

umfassende Informationen zum Clusterstatus bereitgestellt. Auf der Registerkarte **Properties** können Sie den Clusternamen ändern und Konfigurations-, Synchronisierungs- und „Health Check"-Einstellungen (Überprüfungseinstellungen) festlegen.

Nach der Definition und Initialisierung eines Clusters müssen Sie angeben, welche IVEs zu dem Cluster hinzugefügt werden. Nachdem ein IVE als vorgesehenes Mitglied angegeben wurde, können Sie es dem Cluster über folgende Komponenten hinzufügen:

- **Webkonsole**

  Wenn ein konfiguriertes IVE als eigenständiges Gerät betrieben wird, können Sie es über seine Webkonsole zu einem Cluster hinzufügen.

- **Serielle Konsole**

  Ein werksseitig eingestelltes IVE können Sie über seine serielle Konsole zu einem Cluster hinzufügen, indem Sie bei der Ersteinrichtung die Minimalinformationen eingeben.

Wenn ein IVE einem Cluster hinzugefügt wird, initialisiert es seinen Status von einem vorhandenen Mitglied, das Sie angeben. Das neue Mitglied sendet eine Nachricht an das vorhandene Mitglied und fordert die Synchronisierung an. Das bestehende Mitglied sendet daraufhin den Systemstatus an das neue Mitglied, wodurch *alle* Systemdaten dieses Geräts überschrieben werden. Wenn sich zu einem späteren Zeitpunkt bei einem der Clustermitglieder der Status ändert, synchronisieren die Clustermitglieder die Daten. Die Kommunikation zwischen Clustermitgliedern ist verschlüsselt, um Angriffe von außerhalb der firmeninternen Firewall zu verhindern. Jedes IVE verwendet das gemeinsame Kennwort zum Entschlüsseln der Nachrichten von anderen Clustermitgliedern. Aus Sicherheitsgründen ist das Clusterkennwort in IVEs nicht synchronisiert. Beachten Sie, dass bei der Synchronisierung das Dienstpaket von dem neuen Knoten empfangen wird, wodurch der Knoten aktualisiert wird, wenn er über ein älteres Dienstpaket ausgeführt wird.

Weitere Informationen finden Sie unter:

Bereitstellen von zwei Einheiten in einem Aktiv/Passiv-Cluster

Die NetScreen Access 1000-, 3000- und 5000-Plattformen können als Clusterpaar im Aktiv/Passiv-Modus bereitgestellt werden. In diesem Modus bearbeitet ein IVE aktiv Benutzeranforderungen, während das andere IVE passiv im Hintergrund ausgeführt wird, um Statusdaten, einschließlich Systemstatus, Benutzerprofil und Protokollmeldungen, zu synchronisieren. Benutzeranforderungen an die Cluster-VIP (virtuelle IP-Adresse) werden an das aktive IVE geleitet. Wird das aktive IVE offline geschaltet, beginnt das Standby-IVE automatisch mit der Bearbeitung der Benutzeranforderungen. Die Benutzer müssen sich nicht neu anmelden. IVE-Sitzungsdaten, die ein paar Sekunden vor der Offline-Schaltung des aktiven Geräts eingegeben wurden, beispielsweise Cookies und Kennwörter, werden jedoch möglicherweise nicht in das aktuelle IVE-Feld synchronisiert. In diesem Fall müssen sich die Benutzer an den Back-End-Webservern neu anmelden.

Die folgende Abbildung zeigt eine IVE-Clusterkonfiguration vom Typ Aktiv/Passiv mit zwei IVEs, für die externe Ports aktiviert sind. Dieser Modus erhöht zwar weder den Durchsatz noch die Benutzerkapazität, bietet jedoch Redundanz, um auf unerwartete Systemausfälle zu reagieren.

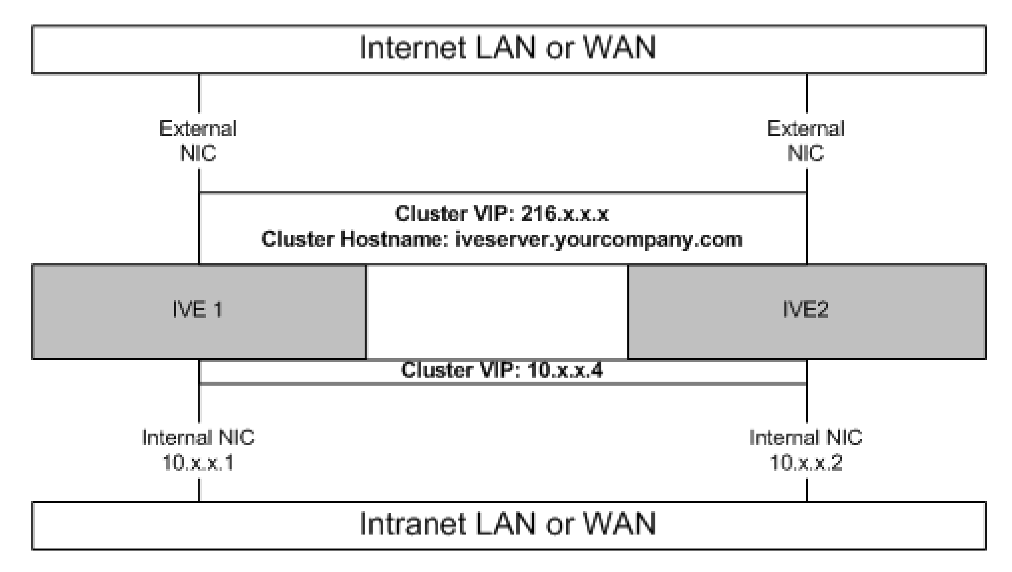


Abbildung 4: Aktiv/Passiv-Clusterpaar
Die Abbildung zeigt einen Aktiv/Passiv-Cluster innerhalb des Netzwerks. IVE-Benutzeranforderungen werden an die Cluster-VIP geleitet, die diese dann an das aktive IVE weiterleitet.

Bereitstellen von zwei oder mehreren Einheiten in einem Aktiv/Aktiv-Cluster

Im Aktiv/Aktiv-Modus verarbeiten alle IVEs im Cluster aktiv die Benutzeranforderungen, die von einem externen Load-Balancer oder nach dem Rotationsprinzip über DNS gesendet wurden. Der Load-Balancer hostet die Cluster-VIP und leitet Benutzeranforderungen auf der Grundlage von SIP-Weiterleitung (Source IP) an ein in seiner Clustergruppe definiertes IVE weiter. Wenn ein IVE offline geschaltet wird, passt der Load-Balancer die Datenlast auf den aktiven IVEs an. Benutzer müssen sich nicht neu anmelden, obwohl einige IVE-Sitzungsdaten, die ein paar Sekunden vor der Offline-Schaltung des aktiven Geräts eingegeben wurden, z. B. Cookies und Kennwörter, möglicherweise nicht auf das aktuelle IVE-Feld synchronisiert wurden. In diesem Fall müssen sich die Benutzer an den Back-End-Webservern neu anmelden.

Der IVE-Cluster selbst führt keine automatischen Failover- oder Lastenausgleichoperationen durch. Er synchronisiert jedoch Statusdaten (System-, Benutzer- und Protokolldaten) zwischen den Clustermitgliedern. Wenn ein offline geschaltetes IVE wieder online geschaltet wird, passt der Load-Balancer die Datenlast erneut an, um sie auf alle aktiven Mitglieder zu verteilen. Dieser Modus bietet gesteigerten Durchsatz und höhere Leistung während Spitzenlastzeiten, verbessert jedoch die Skalierbarkeit über die Gesamtzahl der lizenzierten Benutzer hinaus nicht.

Das IVE hostet eine HTML-Seite, die den Dienststatus für jedes IVE in einem Cluster zur Verfügung stellt. Externe Load-Balancer können anhand dieser Ressource ermitteln, wie die Datenlast effektiv auf die Clusterknoten verteilt werden kann.

So führen Sie die L7-Überprüfung für einen Knoten aus:

- Über einen Browser – Geben Sie folgenden URL ein:

  https://<IVE-Hostname>/dana-na/healthcheck/healthcheck.cgi

- Über einen externen Load-Balancer – Konfigurieren Sie eine Überprüfungsrichtlinie, die die folgende Anforderung an Clusterknoten sendet:

  GET /dana-na/healthcheck/healthcheck.cgi HTTP/1.1\nHost: localhost

  Der Knoten gibt einen der zwei folgenden Werte zurück:

  - Zeichenfolge „Cluster Enabled“ – Der Knoten ist aktiv
  - 500 – Fehler: Leiten Sie keine weiteren Benutzeranforderungen an den Knoten weiter

Die folgende Abbildung zeigt eine IVE-Clusterkonfiguration vom Typ Aktiv/Aktiv, bei der externe Ports für die IVEs aktiviert sind.

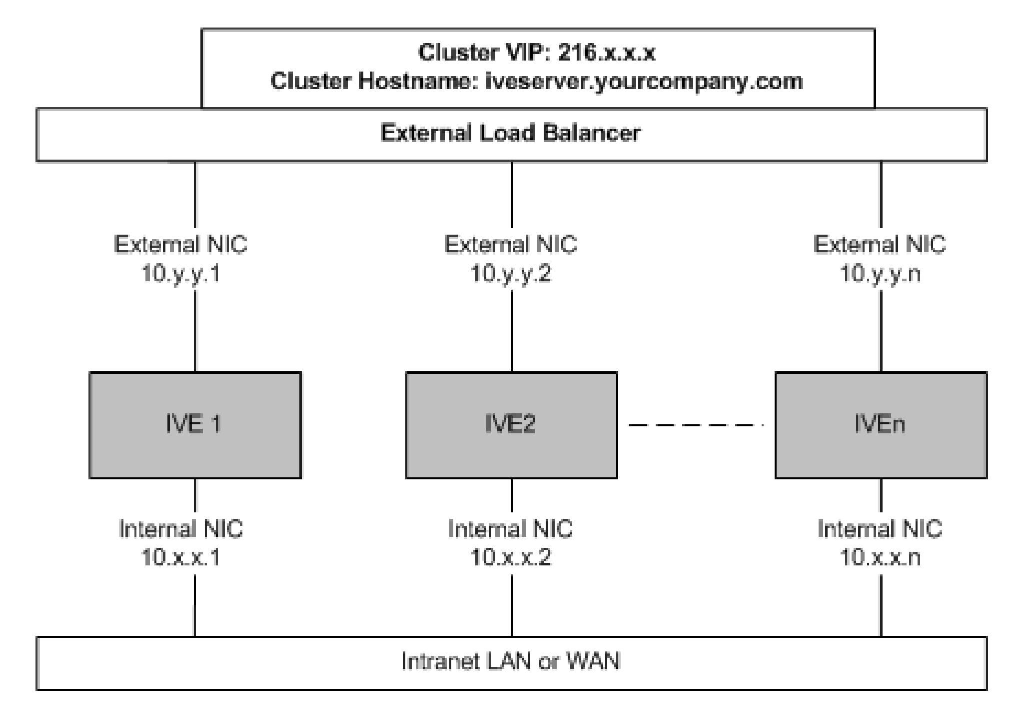


Abbildung 5: Aktiv/Aktiv-Konfiguration
Diese Abbildung zeigt eine Aktiv/Aktiv-Clusterkonfiguration, die hinter einem externen Load-Balancer bereitgestellt wird. Im Aktiv/Aktiv-Modus können Sie ein Clusterpaar oder einen Multi-Unit-Cluster bereitstellen. IVE-Benutzeranforderungen werden an die im Load-Balancer festgelegte Cluster-VIP geleitet, von wo aus sie an das entsprechende Gerät weitergeleitet werden.

Statussynchronisierung

Die Synchronisierung des IVE-Status erfolgt nur über die internen Netzwerkkarten, daher muss jedes Clustermitglied das Clusterkennwort besitzen, um mit anderen Mitgliedern kommunizieren zu können. Die Clustermitglieder synchronisieren Daten, wenn bei einem der Mitglieder des Clusters eine Statusänderung erfolgt. IVE-Clusterstatusdaten sind entweder ***permanent***, d. h. dauerhaft, im IVE gespeichert, oder sie sind nur ***vorübergehend***, d. h. für die Dauer der Benutzersitzung im IVE gespeichert. IVE-Statusdaten untergliedern sich in die folgenden Hauptkategorien:

- **Systemstatus** – Dieser Status ist permanent und ändert sich nicht häufig.
  - Netzwerkeinstellungen
  - Authentifizierungsserver-Konfiguration
  - Konfiguration von Autorisierungsgruppen, zum Beispiel Zugriffssteuerungsliste, Lesezeichen, Nachrichtenübermittlung und Anwendungsdaten
- **Benutzerprofil** – Diese Daten können permanent oder temporär sein, je nachdem, ob beständige Cookies und permanente Kennwortzwischenspeicherung aktiviert sind. Wenn keine dieser Funktionen aktiviert ist, sind die Daten vorübergehend und fallen in die nächste Kategorie.
  - Benutzerlesezeichen – permanent
  - Permanente Benutzercookies – Wenn die Funktion für permanente Cookies aktiviert ist, speichert das IVE Benutzercookies für Websites, die permanente Cookies ausgeben.
  - Permanente Benutzerkennwörter – Wenn die Funktion zum Zwischenspeichern von Kennwörtern aktiviert ist, können Benutzer festlegen, dass ihre Anmeldeinformationen für Anwendungen und Websites gespeichert werden.
- **Benutzersitzung** – Dieser Status ist vorübergehend und dynamisch. Die Benutzersitzungsdaten umfassen Folgendes:
  - Das IVE-Sitzungscookie des Benutzers
  - Vorübergehende Benutzerprofildaten, zu denen Cookies und Kennwörter zählen, die nur während der Benutzersitzung gespeichert werden.
- **Überwachungsstatus** – Dieser permanente Status ist dynamisch und besteht aus Protokollmeldungen[1].

Das IVE ist für die Synchronisation von Daten zwischen Clustermitgliedern verantwortlich, unabhängig davon, ob Sie einen Cluster im Aktiv/Passiv-Modus oder im Aktiv/Aktiv-Modus bereitstellen. Das IVE synchronisiert alle Systemdaten, Benutzerprofildaten und das IVE-Benutzersitzungscookie sofort. Wenn ein Clustermitglied offline geschaltet wird, müssen sich die Benutzer daher nicht erneut am IVE anmelden. Wenn das IVE Benutzersitzungsprofile synchronisiert und Statusdaten überwacht, tritt eine geringfügige Latenz auf. Falls ein Mitglied offline geschaltet wird, kann es passieren, dass sich der Benutzer bei manchen Back-End-Webanwendungen anmelden muss und Administratoren keinen Zugriff auf die Protokolle auf dem ausgefallenen Computer haben.

1. Wenn Sie ein IVE zu einem Cluster hinzufügen, sendet der Clusterleiter keine Protokollmeldungen an das neue Mitglied. Protokollmeldungen werden nicht zwischen Clustermitgliedern synchronisiert, wenn ein Mitglied seinen Dienst wieder aufnimmt oder ein offline geschaltetes IVE wieder online geschaltet wird. Sobald alles IVEs online sind, werden die Protokollmeldungen jedoch synchronisiert.

Sie können auch Synchronisierungseinstellungen konfigurieren, um die Leistung zu verbessern:

- **Angeben des Synchronisationsprotokolls**

  Wenn Sie drei oder mehr IVEs in einen Cluster mit mehreren Einheiten oder mehreren Sites betreiben, können Sie das Synchronisierungsprotokoll auswählen, das der Konfiguration Ihrer Netzwerkhardware am besten entspricht:

  - **Unicast**

    Das IVE sendet an alle Knoten im Cluster die gleiche Meldung. (Dies ist das einzige Synchronisierungsprotokoll, das für Cluster mit zwei Knoten und Multisite-Cluster verfügbar ist.)

  - **Multicast**

    Das IVE sendet eine Meldung an alle Clusterknoten im Netzwerk.

  - **Broadcast**

    Das IVE sendet eine Meldung an alle Geräte im Netzwerk, wobei nicht zum Cluster gehörige Knoten die Meldung löschen.

  Hinweis: Die auf der Cluster-Eigenschaftenseite konfigurierte Einstellung für die Datenübertragung wird nur von den Mitgliedern derselben Site (desselben Subnetzwerks) verwendet. Beispielsweise können Sie in einer Cluster-Site mit 4 Knoten die Multicast-Synchronisierungsmethode festlegen. Die betreffende Site kann jedoch nur mit Sites kommunizieren, die die Unicast-Methode anwenden.

- **Angeben, ob Protokollmeldungen synchronisiert werden sollen**

  Protokollmeldungen können zu umfangreicher Belastung des Netzwerks führen und die Clusterleistung beeinträchtigen. Wir empfehlen, diese Option zu deaktivieren, insbesondere bei einer Multi-Unit-Konfiguration.

Bereitstellen eines Clusters in einer Access Series FIPS-Umgebung

Neben der Freigabe von Status-, Benutzerprofil-, Benutzersitzungs- und Überwachungsstatusdaten können Mitglieder eines Access Series FIPS-Clusters auch Security World-Daten gemeinsam nutzen. Alle Clustermitglieder verwenden gemeinsam denselben privaten Schlüssel, und sie sind über dieselben Administratorkarten zugänglich. Da für das Ändern einer Security World der physische Zugriff auf ein Kryptographiemodul erforderlich ist, können Access Series FIPS-Clustermitglieder jedoch nicht alle ihre Daten im Rahmen des standardmäßigen IVE-Synchronisierungsvorgangs freigeben. Stattdessen muss zum Erstellen eines Access Series FIPS-Clusters Folgendes ausgeführt werden:

1. **Erstellen Sie einen Cluster von Access Series FIPS-Geräten über die Webkonsole.**

   Wie bei einem standardmäßigen IVE-Cluster wird jeder Clusterknoten in einem Access Series FIPS-Cluster mit den Systemstatusdaten vom angegebenen Clustermitglied initialisiert, wobei alle vorhandenen Daten auf dem Knotengerät überschrieben werden.

2. **Aktualisieren Sie die Security World auf jedem Gerät manuell.**

   Nach dem Erstellen eines Clusters müssen Sie jeden Clusterknoten mit der Security World des angegebenen Mitglieds initialisieren. Dazu verwenden Sie eine bereits für die Security World initialisierte Administratorkarte, einen Smartcardleser und die serielle Konsole.

Wenn Sie eine vorhandene Security World in einem Cluster ändern möchten, müssen Sie das Kryptographiemodul der einzelnen Clustermitglieder mithilfe einer Administratorkarte, eines Smartcardlesers und der seriellen Konsole des IVE aktualisieren. Anweisungen hierfür finden Sie in Anhang A: auf Seite 567.

Delegierte Administration – Übersicht

Das IVE-Zugriffsverwaltungssystem ermöglicht Ihnen das Delegieren unterschiedlicher IVE-Verwaltungsaufgaben an verschiedene Administratoren mithilfe von Administratorrollen[1]. Eine ***Administrator-rolle*** ist eine definierte Einheit, die Verwaltungsfunktionen und Sitzungseigenschaften des IVE für Administratoren angibt, die der Rolle zugeordnet sind. Sie können eine Administratorrolle anpassen, indem Sie die Funktionen, Benutzerrollen, Authentifizierungsbereiche und Ressourcenrichtlinien für das IVE auswählen, die Mitglieder der Administratorrolle anzeigen und verwalten dürfen. Beachten Sie, dass delegierte Administratoren nur Rollen, Bereiche und Ressourcenrichtlinien für Benutzer verwalten dürfen. Sie sind jedoch nicht berechtigt, Administratorkomponenten zu verwalten.

Sie können z. B. eine Administratorrolle mit der Bezeichnung „Helpdesk-Administratoren" erstellen und dieser Rolle Benutzer zuweisen, die für die Annahme von Supportfragen der Ebene 1 verantwortlich sind. Dazu gehört z. B. der Support für Benutzer, die nicht auf eine Webanwendung oder IVE-Seite zugreifen können. Für die Problembehebung können die Einstellungen für die Rolle „Helpdesk-Administratoren" wie folgt vorgenommen werden:

- Gewähren Sie den Helpdesk-Administratoren Schreibzugriff auf die Seite **System > Log/Monitoring**, damit sie IVE-Protokolle anzeigen und filtern, kritische Ereignisse in Sitzungsverläufen einzelner Benutzer verfolgen und die Seite **Maintenance > Troubleshooting** anzeigen und somit die Probleme auf einzelnen Benutzersystemen ermitteln können.
- Gewähren Sie den Helpdesk-Administratoren Lesezugriff auf die Seiten **User > Roles**, damit sie darüber informiert sind, welche Lesezeichen, Freigaben und Anwendungen den Rollen der einzelnen Benutzer zur Verfügung stehen, und sie außerdem die Seiten **Resource Policy** und somit die Richtlinien anzeigen können, die einzelnen Benutzern den Zugriff auf ihre Lesezeichen, Freigaben und Anwendungen verweigern.
- Verweigern Sie den Helpdesk-Administratoren Zugriff auf die restlichen Seiten **System** und **Maintenance**, die hauptsächlich zum Konfigurieren von Systemeinstellungen (Installation von Lizenzen und Dienstpaketen) und nicht zur Behebung von einzelnen Benutzerproblemen verwendet werden.

1. Neben evtl. von Ihnen erstellten delegierten Administratorrollen verfügt das IVE über zwei Grundtypen von Administratoren: Superadministratoren (Rolle „.Administrators"), die alle Administrationsaufgaben über die Webkonsole ausführen dürfen, und Administratoren mit Lesezugriff (Rolle „.Read-only Administrators"), die die gesamte IVE-Konfiguration auf der Webkonsole anzeigen, jedoch nicht ändern dürfen. Superadministratoren und Administratoren mit Lesezugriff sind in allen IVE-Produkten verfügbar.

Verwenden Sie die Einstellungen auf der Seite **Administrators > Delegation** (Seite 355), um andere Administratorrollen zu erstellen und deren Zugriff auf die Webkonsole anzupassen.

E-Mail-Client – Übersicht

Die vom IVE bereitgestellte E-Mail-Unterstützung hängt von den optionalen Funktionen ab, die für den IVE-Server lizenziert sind:

- **Secure Email Client Aktualisierungsoption**

  Wenn Sie über die Aktualisierungsoption Secure Email Client verfügen, unterstützt das IVE IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol). Sie können den Zugriff auf die IMAP/POP/SMTP-Mailserver der Firma ganz einfach aktivieren, indem Sie den Mailserver, die E-Mail-Sitzung und die Authentifizierungsinformationen auf der Seite **Resource Policies > Email Settings** (Seite 520) angeben.

- **Secure Application Manager Aktualisierungsoption**

  Wenn Sie über die Aktualisierungsoption Secure Application Manager verfügen, unterstützt das IVE das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll. Sie können den Zugriff auf Microsoft Exchange Server und Lotus Notes Server auf der Seite **User > Roles > SAM > Applications** (Seite 415) aktivieren.

  Wichtig: Wenn der IVE-Server mit der Aktualisierungsoption **Secure Application Manager** lizenziert ist, die das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll unterstützt, trifft dieser Abschnitt nicht zu.

Die Aktualisierungsoption Secure Email Client bietet Benutzern die Möglichkeit, mit standardbasierten E-Mail-Clients sicher von Remotestandorten auf firmeninterne E-Mail-Nachrichten zuzugreifen, ohne dass weitere Software (z. B. ein VPN-Client) benötigt wird. Der IVE-Server funktioniert mit jedem Mailserver, der IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol) unterstützt. Hierzu zählen auch Microsoft Exchange Server und Lotus Notes Mail Server, die IMAP4/POP3/SMTP-Schnittstellen zur Verfügung stellen.

Der IVE-Server befindet sich zwischen dem Remoteclient und dem Mailserver und fungiert als sicherer E-Mail-Proxy. Der Remoteclient verwendet den IVE-Server als (virtuellen) Mailserver und sendet E-Mail über das SSL-Protokoll. Der IVE-Server beendet SSL-Verbindungen des Clients und leitet den entschlüsselten E-Mail-Verkehr innerhalb des LAN an den Mailserver weiter. Der IVE-Server wandelt den unverschlüsselten Datenverkehr des Mailservers dann in S-IMAP (Secure IMAP)-, S-POP (Secure POP)- und S-SMTP (Secure SMTP)-Datenverkehr um und sendet ihn über SSL an den E-Mail-Client.

Weitere Informationen finden Sie unter:

Auswählen eines E-Mail-Clients

Das IVE unterstützt die folgenden E-Mail-Clients:

- Outlook 2000 und 2002
- Outlook Express 5.5 und 6.x
- Netscape Messenger 4.7x und Netscape Mail 6.2

Benutzer, die Remotezugriff auf E-Mail-Nachrichten benötigen, können normalerweise in zwei Kategorien eingeteilt werden:

- **Laptopbenutzer in der Firma**

  Diese Benutzer verwenden im Büro und unterwegs das gleiche Laptop.
- **Benutzer mit Heimcomputern**

  Diese Benutzer verwenden zu Hause einen anderen Computer als im Büro.

Bevor Sie Benutzern einen E-Mail-Client empfehlen, sollten Sie die folgenden Abschnitte lesen, in denen erläutert wird, wie die unterstützten Clients mit folgenden Komponenten interagieren:

- Standardbasierte Mailserver wie Lotus Notes Mail Server (Seite 90)
- Microsoft Exchange Server (Seite 91)

Hinweis: Anleitungen zum Konfigurieren der unterstützten E-Mail-Clients finden Sie auf der Supportsite.

Arbeiten mit einem standardbasierten Mailserver

Das IVE funktioniert mit Mailservern, die IMAP4, POP3 und SMTP unterstützen.

IMAP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können jeden der sechs unterstützen E-Mail-Clients verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf den IVE-Server verweist.
- **Benutzer mit Heimcomputern**: Die Benutzer können für den Remotezugriff auf den IMAP-Server über das IVE jeden der sechs unterstützten E-Mail-Clients verwenden.

POP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können einen der vier Outlook-E-Mail-Clients* verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf den IVE-Server verweist.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf den POP-Server über das IVE einen der vier Outlook-E-Mail-Clients* verwenden.

*Die Netscape-E-Mail-Clients können nicht im POP-Modus für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll wird jedoch vom IVE-Server für die sichere Datenübertragung gefordert.

Arbeiten mit Microsoft Exchange Server

Microsoft Exchange Server unterstützt:

- Systemeigene MAPI-Clients (Messaging Application Programming Interface)
- IMAP-Clients
- POP-Clients
- Outlook Web Access (OWA)

Der IVE-Server bietet Zugriff auf Microsoft Exchange Server über IMAP- und POP-Clients unter Verwendung der Aktualisierungsoption für den Secure Email Client und über OWA mit der Funktion für sicheres Webbrowsing.

Wenn Sie den Zugriff auf Microsoft Exchange Server über das systemeigene MAPI-Protokoll ermöglichen möchten, muss das IVE mit den Aktualisierungsoption für Secure Application Manager lizenziert sein.

Exchange Server und IMAP-Clients

Falls es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- **Laptopbenutzer in der Firma:** Diese Benutzer können einen der Outlook Express- oder Netscape-Clients für den Remotezugriff auf Exchange Server über das IVE verwenden.[1]
- **Benutzer mit Heimcomputern:** Diese Benutzer können einen der sechs unterstützten E-Mail-Clients für den Remotezugriff auf Exchange Server über das IVE verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

Wenn Benutzer die Outlook Express- oder Netscape-Clients im IMAP-Modus ausführen, beachten Sie bitte das folgende Verhalten bei der Ordnerverwaltung:

- **Bei Verwendung von Outlook Express-E-Mail-Clients**

  Gelöschte E-Mail-Nachrichten werden im Posteingang von Outlook Express durchgestrichen angezeigt. Sie werden nicht in den Ordner **Gelöschte Objekte** auf dem Exchange Server verschoben, wie es bei Verwendung des Outlook 2000- oder 2002-Clients der Fall ist. Wenn ein Benutzer gelöschte E-Mail-Nachrichten in einem Outlook Express-Client entfernt, werden die E-Mail-Nachrichten endgültig gelöscht. Wir empfehlen Benutzern von Outlook Express die folgende Vorgehensweise:

  - Zu löschende E-Mail-Nachrichten sollten manuell in den unter **Lokale Ordner** angeordneten Ordner **Gelöschte Objekte** verschoben werden (hierbei handelt es sich um Standardordner). Dieser Ordner wird mit dem Ordner **Gelöschte Objekte** auf dem Exchange Server synchronisiert, sodass Benutzer gelöschte E-Mail-Nachrichten später abrufen können.
  - Sie sollten die gelöschten E-Mail-Nachrichten zunächst im Posteingang von Outlook Express lassen und sie dann bei der nächsten Anmeldung bei Outlook 2000 oder 2002 in den Ordner **Gelöschte Objekte** verschieben.

1. Der Outlook 2000-Client unterstützt nur eine Mailserverkonfiguration, in diesem Fall den systemeigenen MAPI-Modus. Dies verhindert, dass Benutzer den gleichen Client für den Remotezugriff verwenden. Der Outlook 2002-Client bietet Unterstützung für gleichzeitige MAPI- und IMAP-Serverkonfigurationen. Er unterstützt jedoch den IMAP-Zugriff nicht, wenn das MAPI-Konto offline ist, und verhindert hierdurch, dass Remotebenutzer E-Mail-Nachrichten abrufen können.

- **Bei Verwendung von Netscape-E-Mail-Clients**

  Gelöschte E-Mail-Nachrichten werden in den **Papierkorbordner** von Netscape verschoben und im Posteingang von Netscape nicht mehr angezeigt. Aus dem Posteingang von Outlook 2000 oder 2002 werden sie jedoch erst dann entfernt, wenn die Benutzer folgendermaßen vorgehen:

  1. Konfigurieren Sie Netscape so, dass gelöschte Nachrichten in den **Papierkorbordner** verschoben werden, und aktivieren Sie die Option zum Leeren des Posteingangs bei Beendigung des Programms.
  2. Sie sollten immer nur eines der Programme ausführen und es nach beendeter Arbeit schließen. Der Posteingang des anderen Programms wird dann mit dem Server synchronisiert, sodass die gleichen Nachrichten angezeigt werden.

  Gesendete E-Mail-Nachrichten werden außerdem in den Netscape-Ordner für gesendete Objekte (oder einen anderen benutzerdefinierten Ordner) verschoben. Wenn Benutzer möchten, das gesendete Nachrichten im Ordner **Gesendete Objekte** von Microsoft Exchange Server angezeigt werden, müssen sie sie manuell aus dem Netscape-Ordner für gesendete Objekte in den Ordner **Gesendete Objekte** ziehen.

Exchange Server und POP-Clients

Wenn es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- **Laptopbenutzer in der Firma:** Diese Benutzer können für den Remotezugriff auf Exchange Server über das IVE einen der unterstützten Outlook Express-Clients* verwenden.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf Exchange Server über das IVE einen der vier Outlook-Clients* verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

*Die Netscape-E-Mail-Clients können nicht im POP-Modus für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll wird jedoch vom IVE-Server für die sichere Datenübertragung gefordert.

Exchange Server und Outlook Web Access

Um auf dem Exchange-Server OWA-Zugriff zur Verfügung zu stellen und es Benutzern zu ermöglichen, über die Webbrowsingfunktion des IVE auf den Exchange-Server zuzugreifen, müssen Sie OWA lediglich im Intranet als Webanwendung bereitstellen. Es ist keine weitere Einrichtung erforderlich, um eine OWA-Implementierung außerhalb des Netzwerks bereitzustellen.

Hinweis: Bei Verwendung des IVE-Servers für den Zugriff auf Outlook Web Access wird der IIS-Webserver für OWA vor Standardangriffen (z. B. Nimda) geschützt und bietet daher erheblich höhere Sicherheit als der Einsatz von OWA direkt über das Internet.

Arbeiten mit Lotus Notes und Lotus Notes Mail Server

Der Lotus Notes Mail Server stellt POP3- und IMAP4-Schnittstellen zur Verfügung, sodass Benutzer E-Mail von einer Lotus Notes-Mailkonfiguration über das IVE abrufen können. Um zu ermitteln, welcher E-Mail-Client sich für die E-Mail-Benutzer im Unternehmen empfiehlt, die Remotezugriff auf den Lotus-Mailserver benötigen, lesen Sie den Abschnitt über die Arbeit mit standardbasierten Mailservern, „Arbeiten mit einem standardbasierten Mailserver“ auf Seite 90.

Handhelds und PDAs – Übersicht

Zusätzlich zur Zugriffsmöglichkeit für Benutzer auf das IVE über Standardarbeitsstationen und Kioske ermöglicht das IVE den Endbenutzern, auf das IVE über verbundene PDAs, Handhelds und Smart Phones zuzugreifen, z. B. i-Mode und Pocket PCs. Wenn von einem Benutzer über ein PDA- oder Handheld-Gerät eine Verbindung hergestellt wird, ermittelt das IVE, welche IVE-Seiten und -Funktionen anzuzeigen sind. Dies erfolgt entsprechend den Einstellungen auf der Seite **System > Configuration > Client Types** der Webkonsole. Standardmäßig gelten für die Einstellungen auf dieser Seite die folgenden Bedingungen, wenn beim Zugriff auf das IVE folgendes Gerät verwendet wird:

- **i-Mode-Gerät**

  Das IVE zeigt Benutzern cHTML-Seiten (Compact HMTL) ohne Tabellen, Bilder, JavaScript, Java oder Frames an. In Abhängigkeit von den über die Webkonsole aktivierten Funktionen können die Endbenutzer das Web durchsuchen, Verknüpfungen für Weblesezeichen erstellen, Einzelanmeldungen für andere Anwendungen ausführen und ihre Einstellungen bearbeiten (darunter Löschen des Caches und Ändern des IVE/LDAP-Kennwortes). Das IVE ermöglicht es i-Mode-Benutzern, durch Verwendung von Zugriffsschlüsseln auf ihrer Telefontastatur sowie durch normales Navigieren per Suche und Auswahl auf unterstützte Funktionen zuzugreifen.

- **Pocket PC-Gerät**

  Das IVE zeigt HTML-Seiten für mobile Geräte mit Tabellen, Bildern, JavaScript und Frames an, verarbeitet aber kein Java. In Abhängigkeit von den über die Webkonsole aktivierten Funktionen können Endbenutzer auf Mobile Notes zugreifen, das Web durchsuchen, Verknüpfungen für Weblesezeichen erstellen, Einzelanmeldungen für andere Anwendungen ausführen und ihre Einstellungen bearbeiten (darunter Löschen des Caches und Ändern des IVE/LDAP-Kennwortes).

Benutzer von PDAs und Handheld-Geräten können nicht auf die Webkonsole oder die meisten erweiterten Optionen des IVE zugreifen. Dies gilt u. a. auf die Dateinavigation, Network Connect, Secure Application Manager, Secure Meeting, Telnet/SSH, E-Mail Client, Hostprüfung und Cachebereinigung, da von PDAs und Handheld-Geräten im Allgemeinen keine für diese Funktionen erforderlichen ActiveX-, Java- oder JavaScript-Steuerelemente unterstützt werden.

Beachten Sie auch, dass i-Mode-Benutzer nicht auf cookiebasierte Optionen wie Sitzungscookies und SiteMinder-Authentifizierung und –Autorisierung zugreifen können, da HTTP-Cookies von den meisten i-Mode-Browsern nicht unterstützt werden. Das IVE schreibt Hyperlinks neu und fügt in den

URL die Sitzungs-ID ein, statt Cookies zu verwenden. Wenn Benutzer auf den URL zugreifen, wird die Sitzungs-ID vom IVE gelesen.

Konfigurieren des IVE für PDAs und Handheld-Geräte

Gehen Sie für eine ordnungsgemäße Konfiguration des IVE für PDAs und Handheld-Geräte folgendermaßen vor:

1. **Aktivieren Sie den Zugriff auf Systemebene.**

   Wenn andere Browser als die im IVE bereitgestellten Standardbrowser verwendet werden sollen, müssen Sie auf der Registerkarte **System > Configuration > Client Types** die Benutzer-Agent-Zeichenfolgen der PDA- und Handheld-Betriebssysteme eingeben, die unterstützt werden sollen (Seite 202). Eine vollständige Liste von im IVE unterstützten PDA- und Handheld-Browsern finden Sie auf der Supportwebsite im Dokument *Supported Platforms*.

2. **Werten Sie Ihre Benutzerrollen und Ressourcenrichtlinien aus.**

   In Abhängigkeit von den aktivierten IVE-Funktionen müssen Sie entweder die vorhandenen Rollen und Ressourcenrichtlinien für PDA- und Handheld-Benutzer ändern oder neue erstellen. Beachten Sie folgende Punkte:

   - Benutzer von mobilen Geräten können nicht auf Rollen oder Richtlinien zugreifen, für die die Hostprüfung oder Cachebereinigung erforderlich ist, da von Handheld-Geräten im Allgemeinen keine für diese Funktionen erforderlichen ActiveX-, Java- oder JavaScript-Steuerelemente unterstützt werden. Auf den folgenden Registerkarten können Sie diese Optionen deaktivieren:
     - **Users > Roles > [Rolle] > General > Restrictions**
     - **Resource Policies > Web > Access> [Richtlinie] > Detailed Rules**
   - Das Lesen langer Rollennamen auf kleinen Bildschirmen kann für Benutzer von mobilen Geräten problematisch sein. Wenn Benutzer beim Anmelden aus einer Liste von Rollen auswählen müssen, können Sie ggf. die Rollennamen auf der Registerkarte **Users > Roles > [Rolle] > General > Overview** abkürzen.
   - Das Lesen langer Lesezeichnnamen auf kleinen Bildschirmen kann für Benutzer von mobilen Geräten problematisch sein. Auf den folgenden Registerkarten können Sie Weblesezeichen bearbeiten:
     - **Users > Roles > [Rolle] > Web > Bookmarks**
     - **Resource Policies > Web > Access> [Richtlinie] > General**
   - Obwohl erweiterte Funktionen wie Dateinavigation und Secure Application Manager bei PDAs und Handhelds nicht unterstützt werden, müssen diese in den von den Benutzern dieser Geräte verwendeten Rollen und Ressourcenrichtlinien nicht deaktiviert

werden. Diese Optionen werden den Benutzern mobiler Geräte vom IVE einfach nicht angezeigt.

3. **Werten Sie Ihre Authentifizierungs- und Autorisierungsserver aus.**

   Das IVE unterstützt mit Ausnahme des Netegrity SiteMinder-Richtlinienservers alle PDA- und Handheld-Benutzer derselben Authentifizierungs- und Autorisierungsserver als Standardbenutzer. SiteMinder ist von Cookies abhängig, die in i-Mode-Browsern nicht unterstützt werden.

4. **Werten Sie Ihre Bereiche aus.**

   In Abhängigkeit von den aktivierten IVE-Funktionen müssen Sie entweder die vorhandenen Bereiche für PDA- und Handheld-Benutzer ändern oder neue erstellen. Beachten Sie folgende Punkte:

   - Benutzer mobiler Geräte können nicht auf das IVE zugreifen, wenn sie sich in einem Bereich anmelden, für den die Hostprüfung oder Cachebereinigung erforderlich ist, da von Handheld-Geräten im Allgemeinen keine für diese Funktionen erforderlichen ActiveX-, Java- oder JavaScript-Steuerelemente unterstützt werden. Sie können diese Optionen auf den Unterregisterkarten der Seite **System > Configuration > Security** deaktivieren.
   - Benutzer mobiler Geräte können sich beim Netegrity SiteMinder-Server nicht authentifizieren. Sie können auf der Registerkarte **Users > Authentication > [Bereich] > General** einen anderen Authentifizierungsserver für den Bereich auswählen.
   - Das Lesen langer Bereichsnamen auf kleinen Bildschirmen kann für Benutzer von mobilen Geräten problematisch sein. Wenn Benutzer beim Anmelden aus einer Liste von Bereichen auswählen müssen, können Sie ggf. die Bereichsnamen auf der Registerkarte **Users > Authentication > [Bereich] > General** abkürzen.

5. **Werten Sie die zu verwendende Anmelderichtlinie aus.**

   Wenn für Pocket PC-Benutzer eine andere Anmeldeseite verwendet werden soll, können Sie diese auf der Registerkarte **System > Signing In > Sign-in Pages** festlegen und anschließend anhand der Optionen auf der Registerkarte **System > Signing In > Sign-in Policies** eine Anmelderichtlinie erstellen, die auf diese Seite verweist. Wenn Sie über die Lizenz „Advanced“ verfügen, können Sie auch eine benutzerdefinierte Anmeldeseite erstellen, indem Sie in der Datei **sample.zip** verfügbare Pocket PC-Vorlagendateien verwenden.

Hostprüfung – Übersicht

Hostprüfung ist ein clientseitiger Agent, der Endpunktsicherheitsprüfungen an Hosts durchführt, die mit dem IVE eine Verbindung herstellen. Sie können die Hostprüfung aufrufen, bevor Sie einem Benutzer eine IVE-Anmeldeseite anzeigen lassen und wenn die Rollenzuordnungsregel oder Ressourcenrichtlinie ausgewertet wird. Das IVE kann eine Überprüfung der Eigenschaften für die Endpunktsicherheit auf Hosts mithilfe der folgenden Verfahren durchführen:

- **Implementierung der NetScreen Hostprüfung einer unterstützten Anwendung für die Endpunktsicherheit**

  Das ActiveX-Steuerelement ruft die Integration der NetScreen Hostprüfung des angegebenen Endpunktsicherheitsprodukts eines Drittanbieters auf und untersucht den Rückgabewert, um festzustellen, ob das Produkt entsprechend den konfigurierten Richtlinien ausgeführt wird. Das IVE unterstützt gegenwärtig die nahtlose Integration der NetScreen Hostprüfung mit folgenden Produkten:

  - Sygate Enforcement API
  - Sygate Security Agent
  - Zone Labs: ZoneAlarm Pro und Zone Labs Integrity
  - McAfee Desktop Firewall 8.0
  - InfoExpress CyberGatekeeper Agent

- **Integration der NetScreen Hostprüfung anhand einer benutzerdefinierten DLL**

  Die NetScreen Hostprüfungs-API ermöglicht Ihnen das Schreiben einer DLL, die benutzerdefinierte clientseitige Überprüfungen ausführt. Sie müssen diese DLL auf jedem Clientcomputer installieren. Die NetScreen Hostprüfung-API-Dokumentation ist auf der Supportsite verfügbar.

- **Attributüberprüfung**

  Das ActiveX-Steuerelement sucht nach den Spuren der angegebenen Anwendung, einschließlich Prozessen, Dateien und Registrierungseinträgen.

Erstellen globaler Richtlinien für die Hostprüfung

Um die Hostprüfung zum Durchsetzen von Richtlinien für die Verwaltung von Endpunktsicherheit verwenden zu können, müssen Sie globale Richtlinien für die Hostprüfung erstellen, die Folgendes angeben:

- **Host Checking Methods**

  Eine ***Methode*** ist die NetScreen Hostprüfung-(NHC)-Implementierung eines Produkts für die Endpunktsicherheit eines Drittanbieters, mit dem bestimmt wird, ob eine Anwendung in Übereinstimmung mit den konfigurierten Richtlinien ausgeführt wird. Gegenwärtig bietet die Hostprüfung Methoden für folgende Produkte:

  - Sygate Enforcement API
  - Sygate Security Agent
  - Zone Labs: ZoneAlarm Pro und Zone Labs Integrity
  - McAfee Desktop Firewall 8.0
  - InfoExpress CyberGatekeeper Agent

- **Rule Settings**

  Eine ***Regel*** ist eine Anforderung, die von einem Client erfüllt werden muss, damit die Hostprüfung eine Rückgabe über einen Erfolg an den IVE ausführen kann. Sie können fünf Typen von Regeln festlegen:

  - **Custom NHC integration**

    Geben Sie mit dieser Regel den Speicherort einer benutzerdefinierten DLL an, die mit der NHC API geschrieben wird. Die Hostprüfung ruft die DLL auf, um benutzerdefinierte clientseitige Überprüfungen auszuführen. Wenn die DLL eine Bestätigung an die Hostprüfung zurückgibt, sieht das IVE die Regel als erfüllt an. Weitere Informationen über die NHC-API finden Sie in der auf der Supportsite verfügbaren API-Dokumentation.

  - **Port check**

    Verwenden Sie diese Regel, um von einem Clientcomputer das Öffnen bzw. Schließen bestimmter Ports für den Benutzerzugriff auf das IVE zu fordern.

  - **Process check**

    Verwenden Sie diese Regel, um vom Clientcomputer das Ausführen bzw. Unterdrücken eines bestimmten Prozesses für den Benutzerzugriff auf das IVE zu fordern.

  - **File check**

    Verwenden Sie diese Regel, um von einem Clientcomputer den Besitz bzw. das Fehlen einer bestimmten Datei für den Benutzerzugriff auf das IVE zu fordern.

- **Registry settings check**

  Verwenden Sie diese Regel, um von einem Clientcomputer das Vorhandensein bestimmter Registrierungseinstellungen für den Benutzerzugriff auf das IVE zu fordern.

Sie können eine beliebige Anzahl von zu verwendenden Methoden und Regeln für die Hostprüfung auswählen, um zu überprüfen, ob ein Client über die erforderlichen Eigenschaften der Endpunktsicherheit verfügt. Diese Regeln werden kombiniert, um die Richtlinie zu erstellen, die von der Hostprüfung auf dem Client überprüft wird. Sie können dann den Zugriff auf das IVE und die Ressourcen durch Forderung einer Hostprüfung einschränken:

- **Richtlinie für Bereichsauthentifizierung**

  Wenn Administratoren versuchen, sich beim IVE anzumelden, wertet das IVE die Authentifizierungsrichtlinie des angegebenen Bereichs aus und ermittelt, ob die Hostprüfung zu den Anforderungen gehört, die vor der Authentifizierung erfüllt sein müssen. Sie können eine Richtlinie für die Bereichsauthentifizierung so konfigurieren, dass die Hostprüfung heruntergeladen wird, die Hostprüfung herunterladen und die für den Bereich festgelegten Hostprüfung-Richtlinien durchsetzen oder konfigurieren, dass keine Hostprüfung erforderlich ist. Der Benutzer muss sich von einem Computer anmelden, der den Hostprüfung-Anforderungen entspricht, die für den Bereich festgelegt wurden. Wenn dies nicht der Fall ist, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und der Benutzer kann nicht auf das IVE zugreifen.

- **Benutzerrolle**

  Wenn das IVE die Liste der zulässigen Rollen ermittelt, die einem Administrator oder Benutzer zugeordnet sind, wertet es die Einschränkungen der einzelnen Rollen aus. Dabei ermittelt es, ob das Gerät des Benutzers für die Rolle bestimmte Richtlinien für die Hostprüfung einhalten muss. Wenn dies der Fall ist und das Gerät des Benutzers die festgelegten Richtlinien für die Hostprüfung nicht einhält, ordnet das IVE den Benutzer dieser Rolle nicht zu.

- **Ressourcenrichtlinie**

  Wenn ein Benutzer eine Ressource anfordert, wertet das IVE die genauen Regeln der Ressourcenrichtlinie aus. Dabei ermittelt es, ob das Gerät des Benutzers für die betreffende Ressource bestimmte Richtlinien für die Hostprüfung einhalten muss. Wenn das Gerät des Benutzers den festgelegten Richtlinien für die Hostprüfung nicht entspricht, verweigert das IVE den Zugriff auf die betreffende Ressource.

Ausführen der Hostprüfung

Wenn Sie die Hostprüfung als Anforderung für eine Rolle oder Ressourcenrichtlinie festlegen möchten, muss der Agent bei der Anmeldung des Benutzers minimal installiert werden. Dies wird in der Authentifizierungsrichtlinie des Bereichs konfiguriert. Nach der Konfiguration lädt das IVE das ActiveX-Steuerelement auf das System des Benutzers herunter. Außerdem müssen Sie systemweite Richtlinien für die Hostprüfung definieren (Registerkarte **System > Configuration > Security > Hostprüfung**), aus denen Sie dann auswählen, wenn Sie eine Anforderung für die Hostprüfung für einen Bereich, eine Rolle oder eine Ressourcenrichtlinie konfigurieren.

Wenn ein Benutzer auf die Anmeldeseite des IVE zugreifen will, versucht das IVE, den Benutzer einer Rolle zuzuordnen. Oder der Benutzer fordert eine Ressource an, und der Hostprüfungs-Agents überprüft anhand der Methoden und Regeln, die Sie in der zugeordneten Richtlinie für die Hostprüfung festgelegt haben, ob der Client die Endpunktsicherheits-anforderungen erfüllt. Das IVE wartet bis zu 120 Sekunden darauf, dass die Hostprüfung eine Bestätigung oder Ablehnung zurückgibt. Nach Ablauf der Höchstdauer zeigt das IVE eine Fehlermeldung an, und der Benutzer wird auf die Anmeldeseite zurückgeleitet.

Wenn die Endpunktsicherheitsprüfung erfolgreich verläuft, zeigt das IVE dem authentifizierten Benutzer die Startseite an, weist ihn der entsprechenden Rolle zu oder führt die in der Ressourcenrichtlinie festgelegte Aktion durch. Schlägt die Prüfung fehl, wenn der Benutzer versucht, auf die Anmeldeseite des IVE zuzugreifen, zeigt das IVE eine Fehlermeldung mit der Information an, dass der Computer nicht der Richtlinie für die Endpunktsicherheit entspricht. Wenn die Prüfung bei der Auswertung einer Rollenzuordnungsregel durch das IVE fehlschlägt, ordnet das IVE den Benutzer nicht der entsprechenden Rolle zu. Schlägt die Prüfung fehl, wenn der Benutzer eine bestimmte Ressource anfordert, führt das IVE die Aktion nicht aus, die in der entsprechenden Ressourcenrichtlinie festgelegt ist.

Unabhängig von Erfolg oder Fehlschlagen verbleibt die Hostprüfung im Verzeichnis `C:\Programme\Neoteris\Host Checker` auf dem Client. Der Agent kann von Benutzern manuell deinstalliert werden, indem in diesem Verzeichnis die Datei `uninstall.exe` ausgeführt wird. Dieses Verzeichnis enthält außerdem eine Protokolldatei, die bei jedem Ausführen der Hostprüfung neu geschrieben wird.

Weitere Informationen zu den Optionen der Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 25.

Protokollierung und Überwachung – Übersicht

IVE-Protokolldateien sind auf dem IVE gespeicherte Textdateien, die zur Verfolgung von Systemereignissen dienen. Das IVE generiert drei Arten von Protokolldateien:

- **Events log** – Diese Protokolldatei enthält eine Reihe von Systemereignissen, wie z. B. Sitzungsabläufe (beispielsweise aufgrund von Leerlauf oder Überschreitung der Sitzungshöchstdauer), Systemfehler und -warnungen, Anforderungen zur Überprüfung der Serververbindung und Benachrichtigungen über einen Neustart des IVE-Dienstes. (Der IVE-Überwachungsprozess prüft in regelmäßigen Abständen den IVE-Server und startet ihn neu, falls das IVE nicht reagiert.)
- **User Access log** – Diese Protokolldatei enthält Informationen über Benutzerzugriffe auf das IVE, einschließlich der Anzahl gleichzeitig angemeldeter Benutzer jeweils nach Ablauf einer Stunde (Anmeldung zur vollen Stunde), Benutzeranmeldungen und -abmeldungen, Dateianforder-ungen durch Benutzer und Webanforderungen.
- **Administrator Access log** – Diese Protokolldatei enthält Administratorinformationen, einschließlich Änderungen des Administrators an den Benutzer-, System- und Netzwerkeinstellungen, beispielsweise Änderungen an der Sitzungshöchstdauer, an der Option zum Aktivieren bzw. Deaktivieren der URL-Navigation und an von Benutzern erstellten Lesezeichen sowie Geräte- und Server-informationen. Außerdem wird bei jeder Anmeldung, Abmeldung oder Änderung von Lizenzen auf dem IVE durch einen Administrator ein Protokolleintrag erstellt.

Auf den Seiten **System > Log/Monitoring** können Sie angeben, welche Ereignisse protokolliert werden, die maximale Dateigröße für das Systemprotokoll festlegen und einstellen, ob Ereignisse zusätzlich zur lokalen Protokollierung auch auf dem Syslog-Server protokolliert werden sollen. Auf den Seiten **System > Log/Monitoring** können Sie die angegebene Anzahl von Ereignissen anzeigen, die Protokolldatei im Netzwerk speichern und den Inhalt der Protokolle löschen.

Wenn eins der Protokolle die konfigurierte maximale Dateigröße (standardmäßig 200 MB) erreicht, werden die aktuellen Daten in eine Sicherungsprotokolldatei verschoben. Dann wird eine neue, leere Datei für alle folgenden (neuen) Protokollmeldungen erstellt. Mithilfe des Protokollbetrachters kann der Administrator die letzten 5000 Protokollmeldungen (Anzeigebeschränkung des Betrachters) anzeigen. Wenn die aktuelle Protokolldatei weniger als 5000 Protokollmeldungen enthält, werden ältere Protokollmeldungen aus der Sicherungsprotokolldatei geöffnet, sodass insgesamt 5000 Protokollmeldungen angezeigt werden. Dabei werden die Protokolldateien wie eine einzige Datei angezeigt, obwohl sie aufgrund der konfigurierten maximalen Dateigröße getrennt gespeichert sind.

Wichtig: Wenn Sie die Protokollmeldungen speichern oder die FTP-Archivierungsfunktion auf der Seite **Maintenance > Archiving** verwenden möchten, wird die Sicherungsprotokolldatei an die aktuelle Protokolldatei angehängt, und beide werden anschließend als eine Protokolldatei heruntergeladen. Wenn die Protokolldateien nicht archiviert oder gespeichert werden, gehen die ältesten Protokollmeldungen (in der Sicherungsprotokolldatei gespeichert) beim nächsten Verschieben der aktuellen Protokolldatei in die Sicherungsprotokolldatei verloren.

Außerdem können Sie das IVE mit einem Netzwerkverwaltungstool wie HP OpenView als SNMP-Agent überwachen. Das IVE unterstützt SNMP v2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die NetScreen-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen.

Hinweis: Zum Überwachen wesentlicher IVE-Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse: http://net-snmp.sourceforge.net/UCD-SNMP-MIB.txt.

Weitere Informationen finden Sie unter:

Schweregrade der Protokolldatei

Ereignisse in den IVE-Protokolldateien für Ereignisse, Benutzerzugriff und Administratorzugriff werden anhand der folgenden Richtlinien hierarchisiert:

- **Critical (Sicherheitsstufe 10)** – Wenn das IVE Benutzer- und Administratoranforderungen nicht bedienen kann oder seine Funktionen für einen Großteil der Untersysteme verliert, wird ein kritisches Ereignis („Critical Event") protokolliert.
- **Major (Sicherheitsstufe 8-9)** – Wenn das IVE seine Funktionen in mindestens einem Untersystem verliert, aber noch auf die Appliance für andere Zugangsmechanismen zugreifen kann, wird ein größeres Ereignis („Major Event") protokolliert.
- **Minor (Sicherheitsstufe 5-7)** – Wenn das IVE einen Fehler findet, der keinem größeren Ausfall in einem Untersystem entspricht, wird ein kleineres Ereignis („Minor Event") protokolliert. Kleinere Ereignisse entsprechen üblicherweise einzelnen fehlgeschlagenen Anforderungen.
- **Info (Sicherheitsstufe 1-4)** – Wenn das IVE eine Benachrichtigungsmeldung anzeigt, ein Benutzer eine Anforderung vornimmt oder ein Administrator eine Änderung durchführt, wird ein Informationsereignis („Informational Event") protokolliert.

Benutzerdefinierte Filterung von Protokolldateien

Mit dem Central Manager-Paket können Sie die Daten in den Protokolldateien für Ereignisse, Benutzerzugriff und Administratorzugriff filtern und formatieren.

Wenn Sie Protokolldateien filtern, speichert das IVE nur die Meldungen, die in der Filterabfrage angegeben wurden. Sie können z. B. eine Abfrage erstellen, die nur Einträge für einen bestimmten IP-Adress-Bereich oder für Benutzer protokolliert, die in einem bestimmten Bereich angemeldet sind. Eine Abfrage wird mithilfe der IVE-Sprache für benutzerdefinierte Ausdrücke erstellt.

Wenn Sie Protokolldateien formatieren, ändert das IVE lediglich das Aussehen der Meldungen entsprechend Ihrer Angaben. Protokollformate wirken sich nicht auf die Auswahl von Daten aus, die das IVE speichert, sondern nur auf die Art, wie das IVE sie anzeigt. Das IVE umfasst

Standard-, WELF- und W3C-Protokollformate, es steht Ihnen jedoch frei, benutzerdefinierte Formate zu erstellen. Benutzerdefinierte Formate können mithilfe der Protokollfelder erstellt werden.

Konfigurationsanweisungen finden Sie unter „Konfigurieren der Seite „Log Monitoring““ auf Seite 249.

Network Connect – Übersicht

Die Aktualisierungsoption Network Connect bietet Benutzern Möglichkeiten zur Verwendung eines VPN ohne Client und stellt somit ein weiteres Verfahren für den Remotezugriff auf Unternehmensressourcen über das IVE dar. Dieses Feature unterstützt alle Modi für den Internetzugang (einschließlich DFÜ-Verbindungen, Breitband und LAN-Szenarien) vom Clientcomputer aus und funktioniert bei Vorhandensein clientseitiger Proxys und Firewalls, die den SSL-Datenverkehr über Port 443 zulassen.

Wenn ein Benutzer Network Connect startet, wird der gesamte Datenverkehr zum und vom Client über den sicheren Network Connect-Tunnel übertragen. Die einzige Ausnahme besteht für Datenverkehr, der von anderen IVE-fähigen Features initiiert wird, z. B. Webbrowsing, Navigieren durch Dateien und Telnet/SSH. Wenn Sie für bestimmte Benutzer keine weiteren IVE-Funktionen aktivieren möchten, erstellen Sie eine Benutzerrolle, für die nur die Option Network Connect aktiviert ist. Achten Sie darauf, dass die Benutzer, die dieser Rolle zugeordnet sind, nicht noch weiteren Rollen zugeordnet sind, die weitere IVE-Funktionen aktivieren.

Beim Ausführen von Network Connect wird der Client wie ein Knoten im Remote-LAN (Unternehmens-LAN) behandelt und im lokalen LAN des Benutzers nicht mehr angezeigt. Das IVE wird als DNS-Gateway für den Client verwendet und verfügt über keine Informationen zum lokalen LAN des Benutzers. Benutzer können jedoch auf ihrem PC statische Routen festlegen, um bei bestehender Verbindung mit dem Remote-LAN weiterhin auf das lokale LAN zugreifen zu können. Da der gesamte PC-Datenverkehr über den Network Connect-Tunnel zu den internen Unternehmensressourcen übertragen wird, müssen Sie darauf achten, dass andere Hosts im lokalen Netzwerk des Benutzers keine Verbindung mit dem PC herstellen können, auf dem Network Connect ausgeführt wird.

Sie können sicherstellen, dass andere Hosts im lokalen LAN eines Remotebenutzers nicht auf die internen Unternehmensressourcen zugreifen können, indem Sie den Benutzerzugriff auf das lokale Subnetz verweigern (dies wird über die Registerkarte **Users > Roles > *Ausgewählte Rolle* > Network Connect** konfiguriert). Wenn Sie keinen Zugriff auf das lokale Subnetz gewähren, beendet das IVE Network Connect-Sitzungen, die von Clients initiiert wurden, auf denen statische Routen festgelegt sind. Sie können festlegen, dass Clients vor dem Starten einer Remotezugriffssitzung auf Netzwerkebene Lösungen für die Endpunktsicherheit ausführen müssen, z.B. eine persönliche Firewall. Mit der Hostprüfung, die auf Hosts, die mit dem IVE eine Verbindung herstellen, Endpunktsicherheitsprüfungen durchführt, kann sichergestellt werden, dass die Clients Endpunktsicherheitssoftware verwenden. Weitere Informationen finden Sie unter „Hostprüfung – Übersicht“ auf Seite 99.

Informationen über die Konfiguration von Ressourcenrichtlinien für Network Connect finden Sie unter „Konfigurieren der Seite „Network Connect““ auf Seite 509.

Ausführen von Network Connect

Der Network Connect-Agent (NC) wird wie folgt ausgeführt:

1. Ein Benutzer meldet sich im IVE an und klickt auf der IVE-Startseite auf die Verknüpfung für **Network Connect**.
2. Anschließend wird vom IVE ein ActiveX-Steuerelement auf den Clientcomputer heruntergeladen, das die folgenden Aktionen ausführt:
    1. Das IVE ermittelt, ob Network Connect installiert ist. Wenn dies nicht der Fall ist, installiert das IVE die erforderliche Software in einem einmaligen Setup.
    2. Der Dienst Network Connect sendet eine Anforderung an das IVE, um die Verbindung mit einer IP-Adresse aus dem zuvor bereitgestellten IP-Pool zu initialisieren.
    3. Das System Tray-Symbol für Network Connect wird auf der Taskleiste angezeigt.
3. Das IVE reserviert zwei IP-Adressen aus dem konfigurieren Pool und weist folgenden Elementen eine eindeutige IP zu:
    - Dem NC-Dienst, der auf dem Client ausgeführt wird.
    - Dem NC-Prozess, der im IVE ausgeführt wird.
4. Der clientseitige Network Connect-Dienst verwendet die zugewiesenen IP-Adressen für die Kommunikation mit dem im IVE ausgeführten Network Connect-Prozess.
5. Der serverseitige Network Connect-Prozess verwendet die zugewiesene IP-Adresse für die Kommunikation mit Unternehmensressourcen.

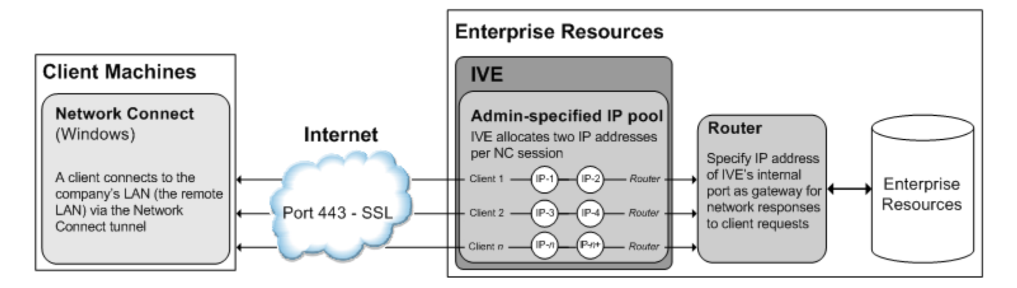


Abbildung 6: Client/Server-Kommunikation mit Network Connect

Der clientseitige Network Connect-Dienst kommuniziert mit dem im IVE ausgeführten serverseitigen Network Connect-Prozess. Dieser Prozess leitet Clientanforderungen an Unternehmensressourcen weiter.

Durchgangsproxy – Übersicht

Mithilfe der Durchgangsproxy-Funktion können Sie Webanwendungen angeben, für die das IVE eine minimale Vermittlung durchführt. Anders als die herkömmliche Antwortproxyfunktion, bei der ebenfalls nur selektive Teile einer Serverantwort neu geschrieben werden, jedoch sowohl Netzwerkänderungen als auch komplexe Konfigurationen vorgenommen werden müssen, müssen Sie für diese Funktion lediglich Anwendungsserver und die Methode angeben, mit der das IVE Clientanforderungen an diese Anwendungsserver empfängt:

- **Über einen IVE-Port**

  Wenn Sie eine Anwendung zur Vermittlung für den Durchgangsproxy angeben, geben Sie einen Port an, an dem das IVE Clientanforderungen an den Anwendungsserver abfragen soll. Wenn das IVE eine Clientanforderung für den Anwendungsserver empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport weiter. Wenn Sie diese Option auswählen, müssen Sie bei Ihrer Firmenfirewall den Datenverkehr für den angegebenen IVE-Port freigeben.

- **Über externe DNS-Auflösung**

  Wenn Sie eine Anwendung zur Vermittlung für den Durchgangsproxy angeben, geben Sie einen Alias für den Hostnamen des Anwendungsservers ein. Für diesen Alias müssen Sie einen Eintrag im externen DNS vornehmen, der für das IVE aufgelöst wird. Wenn das IVE eine Clientanforderung für den Alias empfängt, leitet er die Anforderung an den für den Anwendungsserver angegebenen Port weiter.

  Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports für den Zugriff auf das IVE eingerichtet wurden. Wenn Sie diese Option verwenden, ist es empfehlenswert, dass jeder Hostnamenalias dieselbe Domänenteilzeichenfolge enthält wie der IVE-Hostname und dass Sie ein Serverzertifikat mit Platzhalter in folgendem Format in das IVE hochladen: `*.domaene.com`.

  Wenn das IVE beispielsweise `iveserver.firmenname.com` lautet, muss der Hostnamenalias im Format `anwserver.firmenname.com` und das Zertifikat mit Platzhalter im Format `*.firmenname.com` angegeben werden. Wenn Sie kein Zertifikat mit Platzhalter verwenden, gibt der Browser eines Clients eine Warnung zu einer Zertifikatsnamenüberprüfung aus, wenn ein Benutzer zu einem Anwendungsserver wechselt, da der Hostnamenalias des Anwendungsservers nicht mit dem Zertifikatsdomänennamen übereinstimmt. Durch dieses Verhalten wird ein Benutzer jedoch nicht daran gehindert, auf den Anwendungsserver zuzugreifen.

Beispiele

Wenn das IVE den Namen `iveserver.firmenname.com` hat und Sie über einen Oracle-Server bei `oracle.firmennetzwerk.net:8000` verfügen, könnten Sie diese Anwendungsparameter bei der Angabe eines IVE-Ports angeben:

```
Server: oracle.firmennetzwerk.net
Port: 8000
IVE Port: 11000
```

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an `iveserver.firmenname.com:11000` gesendet wurde, leitet es den Verkehr an `oracle.firmennetzwerk.net:8000` weiter.

Wenn Sie einen Hostnamenalias angeben möchten, können Sie die Anwendung mit folgenden Parametern konfigurieren:

```
Server: oracle.firmennetzwerk.net
Port: 8000
IVE Alias: oracle.firmenname.de
```

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an `oracle.firmenname.de` gesendet wurde, leitet es den Datenverkehr an `oracle.firmennetzwerk.net:8000` weiter.

Wenn Sie Clientanforderungen an das IVE anhand des Hostnamenalias weiterleiten, müssen Sie das IVE außerdem dem externen DNS-Server hinzufügen. Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports für interne Server oder Server in der DMZ gelten.

Ebenso wie das eigentliche Vermittlungsmodul bietet die Durchgangsproxy-Option eine höhere Sicherheit als Secure Application Manager, da das IVE dem Client bei Aktivierung für eine Anwendung ermöglicht, nur Layer-7-Verkehr an feste Anwendungsports an das Firmennetzwerk zu senden. Wenn diese Option aktiviert ist, kann das IVE Anwendungen mit Komponenten unterstützen, die nicht mit dem Modul für die Inhaltsvermittlung kompatibel sind, beispielsweise Java-Applets in Anwendungen der Oracle E-Business Suite oder Applets, die auf einer nicht unterstützten Java Virtual Machine ausgeführt werden.

Hinweis: Die Option des Durchgangsproxys kann nur bei Anwendungen verwendet werden, die feste Ports abfragen und bei denen der Client keine direkten Socketverbindungen herstellt.

Informationen zum Angeben von Anwendungen, für die das IVE eine minimale Vermittlung durchführt, finden Sie unter „Schreiben einer Ressourcenrichtlinie für Durchgangsproxys“ auf Seite 458.

Secure Application Manager – Übersicht

Die Aktualisierungsoption Secure Application Manager ermöglicht sicheren Remotezugriff von Clientanwendungen auf Unternehmensserver auf Anwendungsebene. Sie können zwei Versionen von Secure Application Manager bereitstellen.

- **Windows-Version (W-SAM)**

  Die Windows-Version von Secure Application Manager ist eine Windows-32-Lösung für die sichere, transparente Umleitung ausgehender TCP-Verbindungen über ein IVE-Gerät für jeweils eine Anwendung oder einen Host. Die W-SAM-Software kann mithilfe eines im IVE gehosteten ActiveX-Steuerelements oder anhand des auf einem Clientcomputer vorinstallierten W-SAM-Startprogramms heruntergeladen und gestartet werden. Weitere Informationen finden Sie unter Anhang : auf Seite 116.

- **Java-Version (J-SAM)**

  Die Java-Version von Secure Application Manager bietet Unterstützung für TCP-Client/Server-Anwendungen mit statischen Ports, einschließlich erweiterter Unterstützung von Microsoft MAPI, Lotus Notes und Citrix NFuse. J-SAM unterstützt zudem NetBIOS, wodurch Benutzer bestimmten geschützten Ressourcen Laufwerke zuordnen können. J-SAM funktioniert fehlerfrei in einer Vielzahl von Netzwerkkonfigurationen, wobei TCP-Client/Server-Anwendungen mit dynamischen Ports, vom Server initiierte Verbindungen oder UDP-Datenverkehr jedoch nicht unterstützt werden. J-SAM reserviert bei der Ausführung 20 bis 30 MB RAM (die genaue Speichermenge hängt vom verwendeten JVM ab) und behält im Fall von aktivierter Zwischenspeicherung auf dem Clientcomputer eine JAR-Datei bei. Weitere Informationen finden Sie unter Anhang : auf Seite 118.

Hinweis: Gegenwärtig wird auf Windows-, Linux- und Macintosh-Plattformen Sun JVM, Version 1.4.1 oder höher, unterstützt. Die MS JVM, die auf Sun JRE, Version 1.1 beruht, wird unter Windows ebenfalls unterstützt.

Windows Secure Application Manager (W-SAM) – Übersicht

Die Windows-Version von Secure Application Manager (W-SAM) ist ein Dienst, der anhand des LSP-Verfahrens (Layered Service Provider) Datenverkehr von Clientanwendungen sichert, die auf einem PC ausgeführt werden. Die LSP-Dienstkomponenten werden auf einem Client-PC wahlweise wie folgt installiert:

- Über ein ActiveX-Steuerelement, das vom IVE heruntergeladen wird, wenn ein Benutzer Secure Application Manager über die IVE-Startseite ausführt, oder:
- über das auf einem Client-PC vorinstallierte skriptfähige W-SAM-Startprogramm. In diesem Fall muss das Installationsprogramm an Benutzer verteilt werden, die auf ihren PCs über Administrator-berechtigungen verfügen, damit W-SAM beim Aufrufen vom Start-programm heruntergeladen und installiert werden kann. (Weitere Informationen finden Sie unter Anhang : auf Seite 427.)

  Wenn sich das Startprogramm auf einem PC befindet, gibt es zwei Möglichkeiten, W-SAM aufzurufen:

  - W-SAM kann über ein Eingabeaufforderungsfenster mithilfe von W-SAM-Befehlszeilenargumenten aufgerufen werden.
  - W-SAM kann durch eine Anwendung oder ein Skript gestartet werden, indem an das Startprogramm entsprechende Parameter übermittelt werden. Beispielsweise kann das W-SAM-Startprogramm kann beim Hochfahren des PCs durch ein PC-Batchdateiskript aufgerufen werden.

  Hinweis: Informationen zu Befehlszeilenargumenten und Rückgabecodes finden Sie in Anhang Anhang F.: auf Seite 641.

Wenn W-SAM aufgerufen wurde[1], werden folgende Daten abgefangen:

- TCP-Verbindungsaufrufe von im IVE konfigurierten Anwendungen
- DNS-Abfragen für im IVE konfigurierten Zielhostnamen

Während einer W-SAM-Sitzung wird ein Statusfenster als Prozess im System Tray ausgeführt. Benutzer können auf dieses Symbol doppelklicken, um den aktuellen Sitzungsstatus und eine Liste von Anwendungen und Hosts anzuzeigen, die für die Vermittlung über Secure Application Manager angegeben sind.

1. Sie können Secure Application Manager so konfigurieren, dass er bei der Anmeldung eines Benutzers automatisch gestartet wird. Benutzer können diese Einstellung über das IVE-Menü **System > Preferences** außer Kraft setzen. Wenn der automatische Start deaktiviert ist, muss Secure Application Manager manuell gestartet werden, indem auf die entsprechende Verknüpfung im IVE-Startseitenmenü geklickt wird.

Client/Server-Kommunikation mithilfe von W-SAM

Die folgende Abbildung verdeutlicht die Interaktion zwischen einer Clientanwendung und dem Server über das IVE.

1. Zum Starten von Windows Secure Application Manager klicken Benutzer auf die IVE-Menüoption für Secure Application Manager. Das IVE lädt das ActiveX-Steuerelement auf den Clientcomputer herunter. Dieses Steuerelement konfiguriert den Clientcomputer zum Ausführen von clientseitigen Diensten (LSP), um den Anwendungsverkehr zu sichern. Das Statusfenstersymbol für den Secure Application Manager wird im System Tray angezeigt.
2. Der Benutzer startet eine vom Administrator festgelegte Anwendung oder initiiert einen Prozess, der Daten von einem angegebenen Host anfordert. Wenn die Clientanwendung oder der Prozess versucht, eine Verbindung mit der Ressource herzustellen, fängt Secure Application Manager die Anforderung ab.
3. Secure Application Manager leitet den Hostnamen über SSL an das IVE weiter. Das IVE löst den Hostnamen auf und gibt die IP-Adresse des Zielhosts an Secure Application Manager zurück.
4. Secure Application Manager konfiguriert automatisch einen Kanal für die Portumleitung. Dazu verwendet er eine vorher bereitgestellte IP-Adresse für den `lokalen Host`.

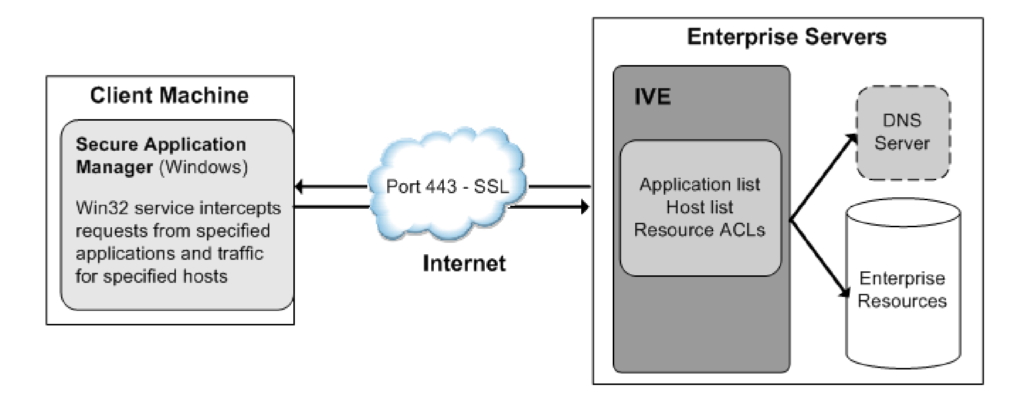


Abbildung 7: Windows Secure Application Manager

Java Secure Application Manager (J-SAM) – Übersicht

Die Java-Version von Secure Application Manager (J-SAM) bietet sichere Portweiterleitung für Anwendungen, die auf einem Remotecomputer ausgeführt werden. Das IVE weist jedem Anwendungsserver, den Sie für einen bestimmten Port festlegen, eine eindeutige IP-Loopbackadresse zu. Wenn Sie beispielsweise für einen einzigen Port Folgendes festlegen:

`app1.eigenefirma.com`, `app2.eigenefirma.com`, `app3.eigenefirma.com, ...`

weist das IVE jeder Anwendung eine eindeutige IP-Loopbackadresse zu:

`127.0.1.10, 127.0.1.11, 127.0.1.12, ...`

Wenn ein Benutzer J-SAM herunterlädt, überwacht J-SAM die vom IVE zugewiesenen Loopbackadressen (am entsprechenden, für den Anwendungsserver festgelegten Clientport) auf Clientanforderungen an die Netzwerkanwendungsserver. J-SAM kapselt die Anforderungsdaten und leitet die verschlüsselten Daten als SSL-Verkehr an das IVE weiter. Das IVE entkapselt die Daten und leitet sie an den festgelegten Serverport auf dem Anwendungsserver im Netzwerk weiter. Der Anwendungsserver gibt seine Antwort an das IVE weiter, das die Daten entkapselt und sie an J-SAM weiterleitet. J-SAM entkapselt anschließend die Antwort des Servers und leitet die Daten an die Clientanwendung weiter. Für die auf dem lokalen Computer ausgeführte Clientanwendung fungiert J-SAM als Anwendungsserver. Für den Anwendungsserver in Ihrem Netzwerk übernimmt das IVE die Rolle der Clientanwendung.

J-SAM stellt außerdem Folgendes bereit:

Client/Server-Kommunikation mithilfe von J-SAM

Die folgende Abbildung verdeutlicht die Interaktion zwischen einer Clientanwendung und dem Server über das IVE. In dieser Abbildung wird vorausgesetzt, dass der Benutzer in der Clientanwendung eine IP-Adresse für `localhost` als Server festlegt.

1. Der Benutzer startet eine auf der Seite **Client Applications** des IVE aufgeführte Clientanwendung. Die Anwendung löst den Remoteserver in `localhost` auf.
2. Die Clientanwendung nimmt Verbindung mit dem auf dem Computer des Benutzers ausgeführten J-SAM auf und beginnt mit dem Senden von Anforderungen.

3. J-SAM kapselt alle Clientanforderungen und leitet diese über SSL an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und leitet sie zum festgelegten Anwendungsserver weiter.
5. Der Anwendungsserver antwortet mit Daten an den IVE-Server.
6. Das IVE kapselt die Antwort und leitet die Antwort vom Anwendungsserver über SSL an J-SAM weiter.
7. J-SAM entkapselt die Anwendungsserverdaten und leitet sie an die Clientanwendung weiter.

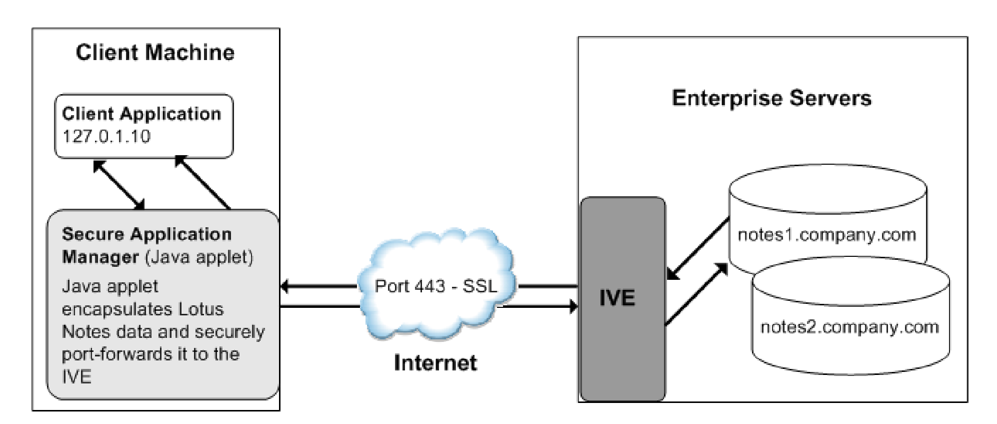


Abbildung 8: Java Secure Application Manager
In dieser Abbildung wird vorausgesetzt, dass der Benutzer in der Clientanwendung eine IP-Adresse für `localhost` als Server festlegt.

Hostnamenauflösung in die Adresse des `lokalen Hosts`

Damit diese Lösung ordnungsgemäß funktioniert, muss eine Clientanwendung auf dem Benutzercomputer den Anwendungsserver in den Client (`localhost`) auflösen, sodass J-SAM die für den Anwendungsserver bestimmten Daten erfassen und über das IVE sicher über Ports leiten kann. J-SAM kann eine automatische Hostzuordnung ausführen, wobei die Datei `hosts` auf dem Client bearbeitet wird, um Anwendungsserver dem `localhost` zuzuordnen. Damit J-SAM die Datei `hosts` eines Benutzers bearbeiten kann, muss der Benutzer über die entsprechenden Rechte auf dem Clientcomputer verfügen:

- **Windows 2000-Benutzer** können einer beliebigen Benutzergruppe angehören. Für die Exchange MAPI-Unterstützung müssen Benutzer jedoch mindestens über die Rechte eines Hauptbenutzers auf dem betreffenden Computer verfügen.
- **Windows XP-Benutzer** müssen über Administratorberechtigungen auf ihren Computern verfügen.
- **Benutzer von Linux (RedHat)** müssen den Browser, in dem J-SAM gestartet wird, als `root` aufrufen.
- **Macintosh-Benutzer** müssen das Administratorkennwort eingeben, wenn Sie von J-SAM eine entsprechende Aufforderung erhalten.

Wenn Benutzer nicht über die entsprechenden Berechtigungen auf ihren Computern verfügen, kann J-SAM die Datei `hosts` nicht automatisch verarbeiten, und die Hostnamenauflösung in den `lokalen Host` findet nicht statt. Benutzer ohne die entsprechenden Berechtigungen haben die folgenden Alternativen:

- Sie können ihren externen DNS-Server zum Auflösen von Anwendungsservern in den `lokalen Host` konfigurieren. Wenn Sie Ihren externen DNS-Server so konfigurieren, dass er die Adresse für einen `lokalen Host` anstelle des Hostnamens des Anwendungsservers verwendet, müssen Remotebenutzer die Reihenfolge, in der ihr Computer nach DNS-Servern sucht, so konfigurieren, dass mit der Firmen-DNS begonnen wird.
- Sie definieren weniger strikte Berechtigungen für das Verzeichnis `etc` und die Datei `etc\hosts`, um J-SAM das Ausführen der notwendigen Änderungen zu ermöglichen.
- Benutzer konfigurieren eines Clientanwendung für die Verwendung der Adresse für den `lokalen Host`, die durch das IVE zugewiesen wurde, in dem in der Regel der Hostname des Anwendungsservers in der Clientanwendung festgelegt wird. Weitere Informationen finden Sie unter Anhang : auf Seite 121.

Zugriff auf privilegierte Ports für Benutzer von Linux und Macintosh

Linux-Benutzer haben keinen Zugriff auf Ports unter 1024, wenn sie auf Ihrem Computer nicht als `root` angemeldet sind. Macintosh-Benutzer haben keinen Zugriff auf Ports unter 1024, es sei denn, sie geben bei einer entsprechenden Aufforderung durch J-SAM das Administratorkennwort ein. So unterstützen Sie Anwendungen, die über privilegierte Ports (Ports unter 1024) ausgeführt werden, beispielsweise eine Telnet-Anwendung:

- Benutzer können den Browser, in dem J-SAM gestartet wird, als `root` starten.
- Sie oder der Benutzer können eine Client-Portnummer ab Port 1024 angeben, wenn Sie die Anwendung der Liste **Client Applications** hinzufügen.

  Wenn beispielsweise für eine Telnet-Anwendung als Clientport 2041 und als Serverport 23 angegeben ist, wird folgender Befehl zum Ausführen der Anwendung verwendet:

  `telnet` *`loopbackIP`* `2041`

  Dabei steht *`loopbackIP`* für die IP-Loopback-Adresse, die dem Anwendungsserver vom IVE zugewiesen wurde. J-SAM überwacht Port 2041 auf Datenverkehr von der Telnet-Anwendung und leitet diesen an das IVE weiter. Das IVE leitet den Datenverkehr dann an Port 23 auf dem Zielserver weiter. Weitere Informationen über das Bestimmen der vom IVE zugewiesenen Loopbackadresse finden Sie unter Anhang : auf Seite 121.

Bestimmen der vom IVE zugewiesenen Loopbackadresse

Benutzer können den Firmen-DNS-Server für Anwendungen nicht ändern, der für die Portweiterleitung hinzugefügt werden. Wenn Sie Benutzern das Angeben von Anwendungen ermöglichen, für die J-SAM als Proxy fungieren soll, müssen diese eine Clientanwendung konfigurieren, um die Adresse des `lokalen Hosts` verwenden zu können, die vom IVE zugewiesen wurde, in dem sie normalerweise den Hostnamen des Servers eingeben. Im Fensterausschnitt **Details** des J-SAM-Browserfensters wird neben dem vom Benutzer angegebenen Port die IP-Loopback-Adresse angezeigt, die vom IVE zugewiesen wird. Um zu bestimmen, welche IP-Adresse das IVE einer auf der Seite **Client Applications** IVE angegebenen Anwendung zuweist, muss ein Benutzer nach dem Hinzufügen der Anwendung Secure Application Manager neu starten. Die der Anwendung zugewiesene Loopbackadresse wird im Fensterausschnitt **Details** des Secure Application Manager-Browserfensters angezeigt:

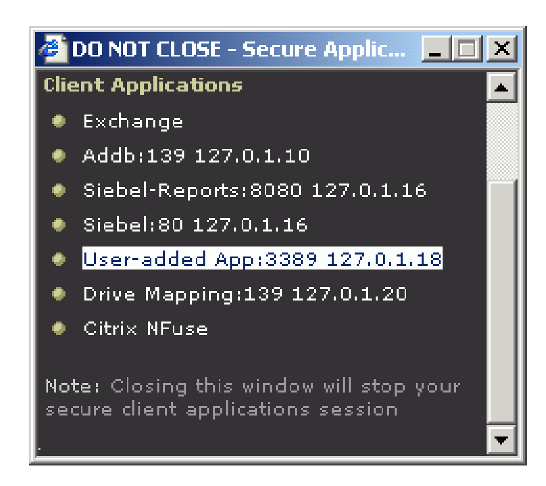


Abbildung 9: **Fensterausschnitt „Details“ des Secure Application Manager (J-SAM)**

In der Clientanwendung muss der Benutzer die vom IVE zugewiesene Loopbackadresse als Anwendungsserver eingeben. Wenn ein Benutzer beispielsweise auf einen Telnet-Server hinter Ihrer Firmenfirewall zugreifen möchte, muss er die folgenden Schritte ausführen:

1. Klicken Sie auf der IVE-Seite **Client Applications** auf **Add Application**.
2. Geben Sie auf der Seite **Add Application** Folgendes an:
   - Im Feld **Remote Server** den vollständig qualifizierten Domänennamen oder die IP-Adresse des Servers, beispielsweise terminalserver.juniper.com.
   - im Feld **Client Port** den Port, der von J-SAM auf Datenverkehr von Clients zum Server überwacht werden soll, beispielsweise 3389.
   - im Feld **Server Port** den Port, den der Remoteserver auf Datenverkehr von der Clientanwendung (J-SAM) überwachen soll, beispielsweise 3389.
3. Klicken Sie auf **Add**, um die Informationen zu speichern.
4. Schließen Sie das **Secure Application Manager**-Browserfenster.
5. Klicken Sie auf der Seite IVE **Client Applications** auf **Start Session**, um Secure Application Manager neu zu starten.
6. Klicken Sie im **Secure Application Manager**-Browserfenster auf **Details**.
7. Sehen Sie auf der Registerkarte **Details** nach, welche Loopbackadresse das IVE dem Remoteserver zugewiesen hat, beispielsweise 127.0.1.18.

8. Geben Sie in der Clientanwendung (beispielsweise Remote Desktop Connection) die Loopbackadresse im Konfigurationsfeld für den Server an. Dieses Feld wird in den einzelnen Anwendungen an unterschiedlicher Stelle angezeigt. Benutzer können diese Angaben über einen Setup-Assistenten oder ein sonstiges Dialogfeld für die Konfiguration eingeben.

Erweiterte Unterstützung für MS Exchange

Remotebenutzer können den Microsoft Outlook-Client auf ihren PCs zum Zugreifen auf E-Mail, ihre Kalender und andere Outlook-Funktionen über das IVE verwenden. Dafür müssen keine Änderungen am Outlook-Client vorgenommen werden, und es ist keine Verbindung auf Netzwerkebene, wie z. B. ein VPN, erforderlich. Diese Funktion erfordert die Installation der Microsoft JVM auf dem Client-PC und wird auf PCs unter Windows 2000 (mit Internet Explorer 5.5 oder 6.0) unterstützt. Diese Funktion ist auch kompatibel mit PCs unter Windows 98 (mit Internet Explorer 5.5) oder Windows XP (mit Internet Explorer 6.0).

Damit diese Funktion von Remotebenutzern verwendet werden kann, muss der im Outlook-Client eingebettete Name der Exchange-Server von den Netzwerkeinstellungen des Benutzer-PCs zum lokalen PC (127.0.0.1, die Standard-IP-Adresse des `localhost`) aufgelöst werden, um einen sicheren Datenverkehr für den Outlook-Client zu gewährleisten. Wir empfehlen, das IVE für die automatische Auflösung von Exchange Server-Hostnamen in `localhost` zu konfigurieren, indem Sie die Datei `hosts` vorübergehend durch die Option für die automatische Hostzuordnung auf einem Clientcomputer aktualisieren.

Client/Server-Kommunikation mithilfe von J-SAM

Die folgende Abbildung beschreibt die Interaktionen zwischen dem Outlook-Client und einem Exchange-Server über das IVE. Diese Abbildung setzt voraus, dass das IVE für die automatische Hostzuordnung konfiguriert ist.

1. Der Benutzer startet den MS Outlook-Client. Outlook versucht, eine Verbindung mit dem Exchange Server `exchange1.ihrefirma.com` herzustellen. Das IVE löst den Hostnamen des Exchange-Servers durch temporäre Änderungen an der Datei `hosts` zu 127.0.0.1 (`localhost`) auf.
2. Outlook stellt eine Verbindung mit Secure Application Manager her, der auf dem PC des Benutzers ausgeführt wird, und beginnt dann, Anforderungen für E-Mail zu senden.
3. Secure Application Manager kapselt alle Anforderungen und leitet diese über SSL vom Outlook-Client an das IVE weiter.

4. Das IVE entkapselt die Clientdaten und sucht in der MAPI-Anforderung nach dem Exchange-Zielserver. Die Anforderung wird dann an den Zielserver weitergeleitet.
5. Jede Anforderung im MAPI-Protokoll codiert den Zielserver für die Anforderung. Wenn von Secure Application Managerstammende MAPI-Anforderungen eingehen, werden sie vom IVE-Server überprüft und jeweils zum entsprechenden Zielserver weiterverteilt. Dieser Prozess wird auch bei Vorhandensein mehrerer Exchange-Server unbemerkt ausgeführt.
6. Der Exchange-Server antwortet dem IVE mit E-Mail-Daten.
7. Das IVE kapselt die Antwort und leitet sie vom Exchange-Server über SSL an Secure Application Manager weiter.
8. Secure Application Manager entkapselt die vom IVE gesendeten Informationen und leitet die normale MAPI-Antwort vom Exchange-Server an dem Outlook-Client weiter.

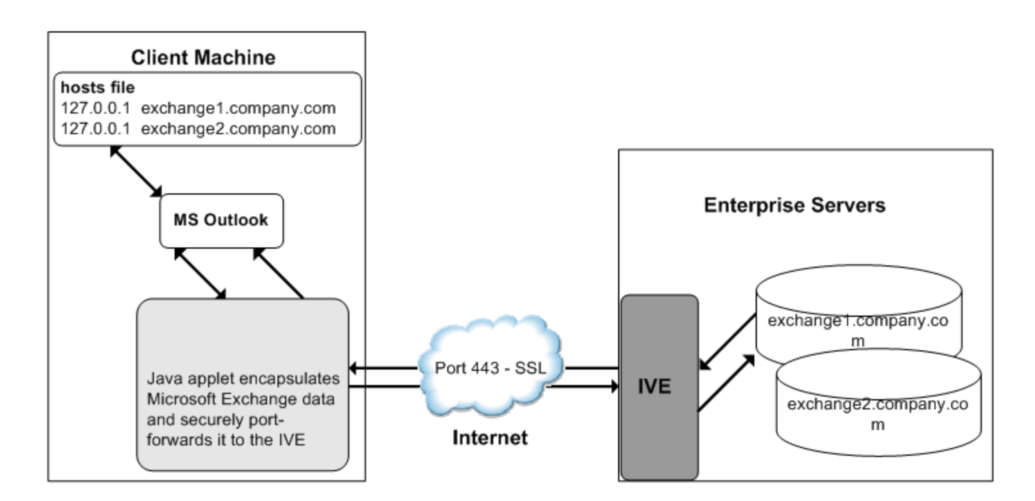


Abbildung 10: Java Secure Application Manager und erweiterte MS Exchange-Unterstützung

In dieser Abbildung wird das für die automatische Hostzuordnung für den MS Outlook-Client konfigurierte IVE dargestellt.

Aktualisierungen der Windows-Registrierung

Beim Start von Secure Application Manager wird die Windows-Registrierungseinstellung `Rpc_Binding_Order` des Benutzers aktualisiert. Diese Einstellung wird der Registrierung hinzugefügt, wenn der Outlook-Client installiert wird, und bestimmt die Protokollsequenz, die der Client zum Kommunizieren mit dem Exchange-Server verwendet.

Der ursprüngliche Wert dieser Einstellung ist:
ncalrpc,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios,ncacn_vns_spp

Nach dem erstmaligen Verwenden von Secure Application Manager ist der Wert:
ncalrpc,ncacn_http,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios,
ncacn_vns_spp

Die Änderung an Rpc_Binding_Order betrifft nur die Ausführung von Secure Application Manager und hat keine anderen Auswirkungen auf dem PC des Benutzers.

Wichtig: Zum Verwenden des Outlook-Client über die Java-Version von Secure Application Manager müssen Benutzer von Windows-PCs über Administratorberechtigungen verfügen.

Erweiterte Unterstützung für Lotus Notes

Remotebenutzer können den Lotus Notes-Client auf ihren PCs zum Zugreifen auf E-Mail, ihre Kalender und andere Funktionen über das IVE verwenden. Dafür müssen keine Änderungen am Lotus Notes-Client vorgenommen werden, und es ist keine Verbindung auf Netzwerkebene, wie beispielsweise ein VPN, erforderlich. Diese Funktion benötigt die Microsoft oder Sun JVM und wird auf PCs unter Windows 2000 (mit Internet Explorer 5.5 oder 6.0) unterstützt.

Client/Server-Kommunikation mithilfe von J-SAM

Damit Remotebenutzer diese Funktion verwenden können, müssen sie den Lotus Notes-Client zum Verwenden von „`localhost`" als Einstellung für den Remotestandort konfigurieren. Secure Application Manager nimmt dann vom Lotus Notes-Client angeforderte Verbindungen auf. Die folgende Abbildung beschreibt die Interaktionen zwischen dem Lotus Notes-Client und einem Lotus Notes-Server über das IVE.

1. Der Benutzer startet den Lotus Notes-Client mit der Home Location-Einstellung. Der Client ermittelt die Proxyeinstellung, d. h. den `localhost`, den PC des Benutzers, für seine Home Location-Einstellung.
2. Der Lotus Notes-Client stellt eine Verbindung mit Secure Application Manager her, und beginnt damit, Anforderungen für E-Mail zu senden.
3. Secure Application Manager kapselt Anforderungen vom Lotus Notes-Client und leitet diese über SSL an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und ermittelt den Lotus Notes-Zielserver in der Lotus Notes-Anforderung. Die Anforderung wird dann an den Zielserver weitergeleitet.

   Jede Anforderung im Lotus Notes-Protokoll codiert den Zielserver für die Anforderung. Wenn Lotus Notes-Anforderungen vom Anwendungsproxy eingehen, ruft der IVE-Server die Zielserverinformationen von den Anforderungen ab und verteilt die Anforderungen an den entsprechenden Zielserver weiter. Deshalb wird diese Funktion auch dann transparent ausgeführt, wenn von einem einzigen Benutzer auf mehrere Lotus Notes-Server zugegriffen wird.
5. Der Lotus Notes-Server antwortet dem IVE mit E-Mail-Daten.
6. Das IVE kapselt die Antwort vom Lotus Notes-Server und leitet diese über SSL an Secure Application Manager weiter.
7. Secure Application Manager entkapselt die vom IVE gesendeten Informationen und leitet die normale Antwort vom Lotus Notes-Server an den Lotus Notes-Client weiter.

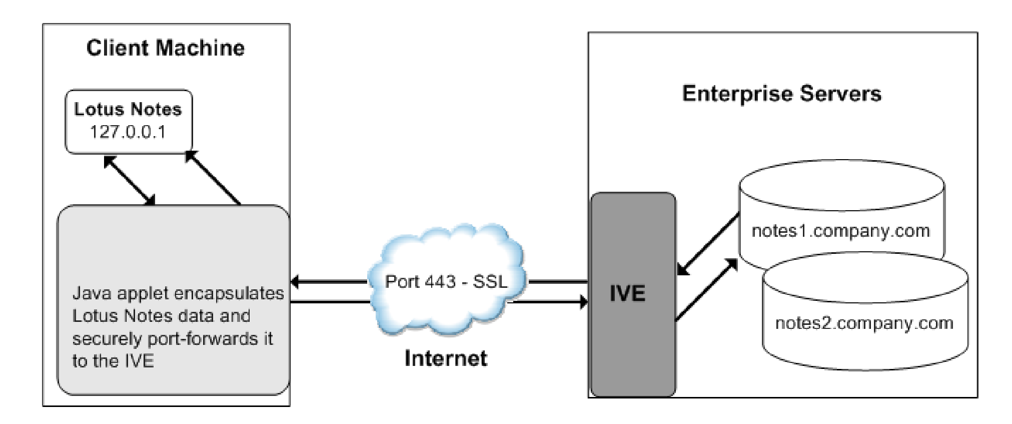


Abbildung 11: Java Secure Application Manager und erweiterte Lotus Notes-Unterstützung

In dieser Abbildung wird der Remotestandortwert des Lotus Notes-Clients dargestellt, der auf dem `localhost` konfiguriert wird.

Erweiterte Unterstützung für Citrix NFuse

Wenn ein Benutzer auf einem NFuse-Server eine Anwendung auswählt, sendet der NFuse-Server eine ICA-Datei an den Client. Wenn das IVE die ICA-Datei überschreibt, ersetzt es Hostnamen und IP-Adressen durch vorher bereitgestellte IP-Adressen des `localhost`. Der ICA-Client sendet dann Anwendungsanforderungen an eine der IP-Adressen des `localhost`. Secure Application Manager kapselt die Daten und sendet sie an das IVE. Das IVE entkapselt die Daten und sendet sie über Port 1494 an den passenden MetaFrame-Server.

Liste unterstützter Versionen

- MetaFrame™-Server: Versionen 1.8, XP 1.0, mit Service Packs 1 und 2
- Nfuse-Webserver: Versionen 1.5, 1.6 und 1.7
- ICA-Clients:
  - Windows 32-Bit: PN-Client Version 6.30 und Webclient Version 7,0
  - Benutzer von Program Neighborhood müssen den Server und die Anwendungen festlegen, auf die sie bei Verwendung des PN-Client zugreifen möchten. Diese Version des IVE unterstützt den Suchmechanismus nicht, über den Anwendungen auf MetaFrame-Servern für Benutzer von Program Neighborhood angezeigt werden.
  - Java: Version 6.2 für den eigenständigen Client und Versionen 6.2 und 6.3 für den Appletmodus. Wenn Sie den Appletmodus des Java-Client verwenden möchten, müssen Sie darauf achten, dass die Unterstützung für Java-Applets unter „Web > General page" aktiviert ist.

Hinweis:

Das IVE bietet eine Alternative zur Bereitstellung von CSG.

Einzelanmeldung – Übersicht

Die Einzelanmeldung (Single Sign-on, SSO) ist ein Vorgang, der es vorauthentifizierten IVE-Benutzern ermöglicht, auf von einem anderen Zugriffsverwaltungssystem geschützte Ressourcen zuzugreifen, ohne die jeweiligen Anmeldeinformationen erneut eingeben zu müssen. Das IVE stellt mehrere SSO-Mechanismen bereit:

- **Remote-SSO**

  Das IVE ermöglicht eine lose Integration von Anwendungen, die statische POST-Aktionen in HTML-Formularen verwenden, um Benutzer anzumelden. Bei ordnungsgemäßer Konfiguration können Sie IVE-Anmeldeinformationen, LDAP-Attribute und Zertifikatattribute in einer webfähigen Anwendung bereitstellen sowie Cookies und Header festlegen, sodass Sie Benutzern den Zugriff auf die Anwendung ohne eine erneute Authentifizierung ermöglichen.

  Zum Aktivieren von SSO für eine Webanwendung müssen Sie eine Webressourcenrichtlinie (URL) über das IVE erstellen. Sie müssen in der Richtlinie den URL der Anmeldeseite der Webanwendung und die IVE-Anmeldeinformationen sowie Headerwerte und Cookies angeben, die Sie an die Anwendung senden müssen. Anschließend müssen Sie den Benutzern innerhalb einer Rolle Zugriff auf die Ressourcenrichtlinie erteilen.

  Weitere Informationen finden Sie unter „Remote SSO – Übersicht“ auf Seite 130.

- **Netegrity SiteMinder-Richtlinienserver**

  Das IVE ermöglicht eine enge Integration des Netegrity SiteMinder-Richtlinienservers. Bei ordnungsgemäßer Konfiguration können Sie IVE-Benutzer mit einem Richtlinienserver authentifizieren und den Benutzern anschließend den Zugriff auf durch SiteMinder geschützte Ressourcen ohne eine erneute Authentifizierung ermöglichen (unter der Voraussetzung, dass sie für die richtige Sicherheitsebene autorisiert sind). Außerdem können Sie Benutzer über das IVE erneut authentifizieren, wenn sie Ressourcen anfordern, für die ihre aktuelle Sicherheitsebene nicht ausreicht. Sie können es den Benutzern auch ermöglichen, sich zuerst am Richtlinienserver anzumelden und dann ohne eine erneute Authentifizierung auf das IVE zuzugreifen.

  Zum Aktivieren von SSO zwischen Netegrity SiteMinder und dem IVE müssen Sie eine SiteMinder-Serverinstanz über das IVE konfigurieren und dem Server anschließend einen Authentifizierungsbereich zuordnen. Allen Benutzern, die sich über den Bereich anmelden, wird die Einzelanmeldung bei durch Netegrity geschützten Ressourcen ermöglicht.

  Weitere Informationen finden Sie unter „Netegrity SiteMinder – Übersicht“ auf Seite 321.

- **SAML**

  Das IVE ermöglicht eine lose Integration von ausgewählten Zugriffsverwaltungssystemen, die für die Kommunikation mit anderen Systemen SAML (Security Assertion Markup Language) verwenden. Bei ordnungsgemäßer Konfiguration können sich die Benutzer beim IVE anmelden und dann ohne eine erneute Authentifizierung auf vom Zugriffsverwaltungssystem geschützte Ressourcen zugreifen.

  Zum Aktivieren von SSO für eine von einem SAML-fähigen System geschützte Ressource müssen Sie eine Webressourcenrichtlinie (URL) über das IVE erstellen. Sie müssen in der Richtlinie eine Vertrauensstellung zwischen dem IVE und dem SAML-fähigen Zugriffsverwaltungssystem herstellen, indem Sie Informationen zu den beiden Systemen bereitstellen und den für die gemeinsame Nutzung von Informationen zu verwendenden Mechanismus angeben. Anschließend müssen Sie den Benutzern innerhalb einer Rolle Zugriff auf die Ressourcenrichtlinie erteilen.

  Weitere Informationen finden Sie unter „SAML – Übersicht“ auf Seite 132.

Remote SSO – Übersicht

Mithilfe der Funktion Remote-SSO (Single Sign-On, Einzelanmeldung) können Sie einen Anmeldeseiten-URL einer Anwendung angeben, an die das IVE die Anmeldeinformationen eines Benutzers senden soll. Dadurch wird vermieden, dass Benutzer ihre Anmeldeinformationen für den Zugriff auf verschiedene Back-End-Anwendungen mehrmals angeben müssen. Sie können außerdem zusätzliche Formularwerte und benutzerdefinierte Header (einschließlich Cookies) angeben, die an das Anmeldeformular einer Anwendung gesendet werden.

Für die Remote-SSO-Konfiguration müssen Webressourcenrichtlinien angegeben werden:

- **Form-POST-Richtlinie**

  Diese Art von Remote-SSO-Richtlinie gibt den Anmeldeseiten-URL einer Anwendung an, an die IVE-Daten und die zu veröffentlichenden Daten gesendet werden sollen. Diese Daten können den IVE-Benutzernamen und das IVE-Benutzerkennwort sowie die Systemdaten enthalten, die in Systemvariablen gespeichert sind („Systemvariablen und Beispiele“ auf Seite 601). Sie können außerdem angeben, ob Benutzer diese Informationen ändern dürfen. Konfigurationsanweisungen finden Sie unter „Registerkarte „Remote SSO > Form POST““ auf Seite 460.

- **Header/Cookies-Richtlinie**

  Diese Art von Remote-SSO-Richtlinie gibt Ressourcen wie benutzerdefinierte Anwendungen an, an die benutzerdefinierte Header und Cookies gesendet werden können. Konfigurationsanweisungen finden Sie unter „Registerkarte „Remote SSO > Headers/Cookies““ auf Seite 462.

Wenn sich die Anmeldeinformationen eines Benutzers von denen unterscheiden, die die Back-End-Anwendung benötigt, kann der Benutzer auch folgendermaßen auf die Anwendung zugreifen:

- **Manuelle Anmeldung**

  Der Benutzer kann schnell auf die Back-End-Anwendung zugreifen, indem er auf der Anmeldeseite der Anwendung seine Anmeldeinformationen manuell eingibt. Der Benutzer kann seine Anmeldeinformationen und sonstige erforderliche Daten auch entsprechend der folgenden Beschreibung über die Seite **Advanced Preferences** dauerhaft im IVE speichern. Dieser Vorgang ist jedoch optional.

- **Angeben der erforderlichen Anmeldeinformationen auf dem IVE**

  Der Benutzer muss für das IVE die Anmeldeinformationen für die Anwendung fehlerfrei angeben. Die Informationen werden auf der Seite **Advanced Preferences** festgelegt. Nach dem Festlegen muss sich der Benutzer abmelden und erneut anmelden, um seine Anmeldeinformationen für das IVE zu speichern. Wenn der Benutzer das nächste Mal auf das Remote-SSO-Lesezeichen klickt, um sich bei der Anwendung anzumelden, sendet das IVE die aktualisierten Anmeldeinformationen.

Hinweis: Übergeben Sie mithilfe der Remote-SSO-Funktion Daten an Anwendungen, in deren HTML-Formularen statische POST-Aktionen enthalten sind. Es empfiehlt sich nicht, Remote-SSO mit Anwendungen zu verwenden, bei denen sich regelmäßig ändernde URL-POST-Aktionen zur Anwendung kommen, ein Ablauf nach einer bestimmten Zeit auftritt oder POST-Aktionen ablaufen, die zum Zeitpunkt der Erstellung des Formulars generiert wurden.

SAML – Übersicht

Mithilfe der SAML-Funktion können Sie Benutzer- und Sitzungsstatusinformationen vom IVE an ein anderes vertrauenswürdiges Zugriffsverwaltungssystem weiterleiten, das SAML (Secure Access Markup Language) unterstützt. ***SAML*** stellt einen Mechanismus für zwei verschiedene Systeme bereit, mit dem Authentifizierungs- und Autorisierungsinformationen mithilfe eines XML-Frameworks erstellt und ausgetauscht werden können, sodass die Notwendigkeit für die Benutzer, ihre Anmeldeinformationen beim Zugreifen auf mehrere Anwendungen oder Domänen erneut einzugeben, minimiert wird[1]. Das IVE verwendet SAML, Version 1.1.

Die SAML-Austauschvorgänge sind von einer Vertrauensstellung zwischen zwei Systemen oder Domänen abhängig. Bei den Austauschvorgängen fungiert ein System als ***SAML-Autorität*** (auch bestätigende Partei oder SAML-Responder genannt), die Informationen zum Benutzer hinterlegt bzw. bestätigt. Das andere System fungiert als ***Relying Party (die sich auf Vertrauenswürdigkeit verlassende Partei)*** (auch SAML-Receiver genannt), die sich auf das von der SAML-Autorität bereitgestellte Statement (auch Assertion genannt) verlässt. Wenn die Relying Party der SAML-Autorität vertraut, authentifiziert oder autorisiert sie den Benutzer auf Grundlage der von der SAML-Autorität bereitgestellten Informationen.

So kann beispielsweise der authentifizierte IVE-Benutzer John Smith versuchen, auf eine von einem Zugriffsverwaltungssystem geschützte Ressource zuzugreifen. Dabei fungiert das IVE als SAML-Autorität und zeigt folgende Meldung an: „This user is John Smith. He was authenticated using a password mechanism“. Das Zugriffsverwaltungssystem (die Relying Party) empfängt dieses Statement und vertraut dem IVE. (Aus diesem Grund wird auch darauf vertraut, dass der Benutzer ordnungsgemäß vom IVE identifiziert wurde.) Es besteht auch die Möglichkeit, dass das Zugriffsverwaltungssystem dem Benutzer den Zugriff auf die angeforderte Ressource verweigert, weil John Smith z. B. nicht über ausreichende Zugriffsrechte für das System verfügt, obwohl es den vom IVE gesendeten Informationen vertraut.

Informationen zum Konfigurieren einer Vertrauensstellung finden Sie unter „Herstellen einer Vertrauensstellung zwischen SAML-fähigen Systemen“ auf Seite 139.

1. Secure Access Markup Language wurde vom SSTC (Security Services Technical Committee) von OASIS-Organisation für Standards entwickelt. Eine technische Übersicht über SAML finden Sie auf der OASIS-Website unter: http://www.oasis-open.org/committees/download.php/5836/sstc-saml-tech-overview-1.1-draft-03.pdf.

Beim Konfigurieren des IVE können Sie SAML für Folgendes verwenden:

- **SSO-Authentifizierung (Single Sign-On, Einzelanmeldung)**

  Im Rahmen einer SAML-SSO-Transaktion wird ein authentifizierter IVE-Benutzer nahtlos in einem anderen System angemeldet, ohne die Anmeldeinformationen erneut bereitstellen zu müssen. Bei diesem Transaktionstyp stellt das IVE die SAML-Autorität dar. Es wird ein so genanntes ***Authentifizierungsstatement*** erzeugt, das den Benutzernamen sowie die Methode der Authentifizierung des Benutzers angibt. Wenn die Relying Party (die bei SAML-SSO-Transaktionen als ***Assertion Consumer Service*** bezeichnet wird) dem IVE vertraut, wird der Benutzer nahtlos im Assertion Consumer Service mit dem im Statement enthaltenen Benutzernamen angemeldet. Weitere Informationen finden Sie unter „Informationen zu SAML-SSO-Profilen“ auf Seite 134.

- **Zugriffssteuerungsautorisierung**

  Im Rahmen einer SAML-Zugriffssteuerungstransaktion ruft das IVE bei einem Zugriffsverwaltungssystem ab, ob der Benutzer über entsprechende Zugriffsrechte verfügt. Bei diesem Transaktionstyp stellt das IVE die Relying Party dar (wird bei Zugriffssteuerungstransaktionen auch als Policy Enforcement Point (PEP) bezeichnet). Das IVE verwendet und erzwingt ein vom Zugriffsverwaltungssystem (SAML-Autorität) bereitgestelltes ***Authorization Decision Statement***, in dem angegeben wird, dass der Benutzer für den Zugriff berechtigt ist. Wenn die SAML-Autorität (die bei Zugriffssteuerungstransaktionen auch als Policy Decision Point, PDP bezeichnet wird) angibt, dass der IVE-Benutzer über ausreichende Zugriffsrechte verfügt, kann der Benutzer auf die gewünschte Ressource zugreifen. Weitere Informationen finden Sie unter „Informationen zu Zugriffssteuerungsrichtlinien“ auf Seite 138.

Zum Konfigurieren von SAML über das IVE müssen Sie eine Webressourcenrichtlinie für einen URL konfigurieren. Sie müssen in der Richtlinie Informationen zum IVE, zum vertrauenswürdigen Zugriffsverwaltungssystem sowie zu dem für die gemeinsame Nutzung von Informationen zu verwendenden Mechanismus bereitstellen. Anschließend müssen Sie den IVE-Benutzern innerhalb einer Rolle Zugriff auf die Ressourcenrichtlinie erteilen. Weitere Informationen finden Sie unter „Registerkarte „SAML > SSO““ auf Seite 464 oder unter „Registerkarte „SAML > Access Control““ auf Seite 470.

Wichtig:

- Das IVE unterstützt keine ***Attributstatements***, in denen bestimmte Details über den Benutzer angegeben werden (z. B. „John Smith is a member of the gold group“).
- Das IVE akzeptiert keine Authentifizierungsstatements von anderen SAML-Autoritäten. Im Rahmen einer SAML-SSO-Transaktion muss sich der Benutzer zuerst beim IVE anmelden.

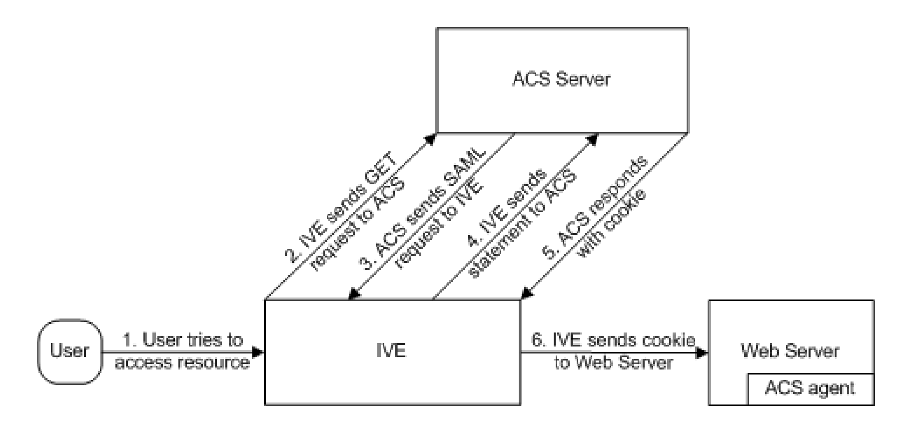
- Das IVE generiert keine Authorization Decision Statements, es verwendet sie nur.
- Das IVE gewährt den Benutzern jedoch nicht nur den Zugriff auf einen URL auf Grundlage des von einer SAML-Autorität zurückgegebenen Authorization Decision Statement. Das IVE ermöglicht Ihnen außerdem das Definieren von Benutzerzugriffsrechten für einen URL mithilfe von IVE-Mechanismen (Registerkarte **Resource Policies > Web > Access**). Wenn Sie Zugriffssteuerungen sowohl über das IVE als auch eine SAML-Autorität definieren, müssen beide Quellen den Zugriff auf einen URL gewähren, damit ein Benutzer darauf zugreifen kann. Sie können beispielsweise eine IVE-Zugriffsrichtlinie konfigurieren, um Mitgliedern der Rolle „Users" den Zugriff auf `www.google.com` zu verweigern, und eine andere SAML-Richtlinie konfigurieren, bei der die Benutzerzugriffsrechte auf einem Attribut in einem Zugriffsverwaltungssystem basieren. Selbst wenn das Zugriffsverwaltungssystem den Benutzern den Zugriff auf `www.google.com` gewährt, wird ihnen jedoch der Zugriff aufgrund der IVE-Richtlinie verweigert.
- Zugriffsverwaltungssysteme, die SAML unterstützen, können auf die Anfrage, ob ein Benutzer auf eine Ressource zugreifen darf, eine Zusage, eine Verweigerung oder eine unbestimmte Antwort zurückgeben. Wenn das IVE eine unbestimmte Antwort erhält, wird dem Benutzer der Zugriff verweigert.
- Es tritt eine Zeitüberschreitung bei der Sitzung auf dem IVE auf, und es ist keine Koordination mit dem Zugriffsverwaltungssystem möglich. Wenn ein Sitzungscookie des Zugriffsverwaltungssystems eines Benutzers vor dem IVE-Cookie (`DSIDcookie`) abläuft, wird die Einzelanmeldung zwischen den zwei Systemen aufgehoben. Der Benutzer muss sich bei einer Zeitüberschreitung im Zugriffsverwaltungssystem erneut anmelden.

Informationen zu SAML-SSO-Profilen

Beim Aktivieren von SSO-Transaktionen für ein vertrauenswürdiges Zugriffsverwaltungssystem müssen Sie angeben, ob das Zugriffsverwaltungssystem Benutzerinformationen vom IVE abrufen soll oder ob das IVE Benutzerinformationen an das Zugriffsverwaltungssystem weiterleiten soll. Sie geben die von den zwei Systemen zu verwendende Kommunikationsmethode an, indem Sie bei der Konfiguration ein Profil auswählen. Ein ***Profil*** wird von zwei vertrauenswürdigen Sites zum Übertragen eines SAML-Statements verwendet. Beim Konfigurieren des IVE können Sie wählen, ob ein Artifact- oder ein POST-Profil verwendet werden soll.

Artifact-Profil

Wenn Sie sich für die Kommunikation mit dem ***Artifact-Profil*** (wird auch als Browser-Artifact-Profil bezeichnet) entscheiden, ruft der vertrauenswürdige Zugriffsverwaltungsserver die Authentifizierungsdaten vom IVE ab. Dies wird im folgenden Diagramm dargestellt:



Das IVE und ein Assertion Consumer Service (ACS) gehen beim Weiterleiten von Informationen folgendermaßen vor:

1. **Der Benutzer möchte auf eine Ressource zugreifen.**

   Ein Benutzer ist beim IVE angemeldet und versucht, auf eine geschützte Ressource auf einem Webserver zuzugreifen.

2. **Das IVE sendet eine HTTP- oder HTTPS GET-Anforderung an den ACS.**

   Das IVE fängt die Anforderung ab und überprüft, ob der erforderliche SSO-Vorgang bereits ausgeführt wurde, um die Anforderung zu berücksichtigen. Ist dies nicht der Fall, erstellt das IVE ein Authentifizierungsstatement und leitet eine HTTP-Abfragevariable (als Artifact bezeichnet) an den Assertion Consumer Service weiter.

   Ein ***Artifact*** ist eine Base-64-codierte Zeichenfolge, die die Quell-ID der Quellsite (eine 20-Byte-Zeichenfolge, die auf das IVE verweist) und eine zufällig erstellte Zeichenfolge enthält, die als Handle für das Authentifizierungsstatement fungiert. (Beachten Sie, dass ein Handle 5 Minuten nach dem Senden des Artifacts abläuft. Wenn also der Assertion Consumer Service nach 5 Minuten antwortet, sendet das IVE kein Statement. Beachten Sie außerdem, dass das IVE ein Handle nach der ersten Verwendung verwirft, um zu vermeiden, dass das Handle ein zweites Mal verwendet wird.)

3. **Der ACS sendet eine SAML-Anforderung an das IVE**.

   Der Assertion Consumer Service verwendet die im vorherigen Schritt gesendete Quell-ID, um die IVE-Adresse zu ermitteln. Anschließend sendet der Assertion Consumer Service eine in einer SOAP-Nachricht enthaltene Statementanforderung an die folgende Adresse auf dem IVE:

   `https://<IVEhostname>/dana-ws/saml.ws`

   Die Anforderung umfasst das im vorherigen Schritt weitergeleitete Statementhandle.

   Wichtig: Das IVE unterstützt nur Artifacts vom Typ 0x0001. Dieser Artifacttyp leitet einen Verweis auf die Adresse der Quellsite (also die Quell-ID des IVE) weiter, statt die eigentliche Adresse zu senden. Zum Verarbeiten von Artifacts vom Typ 0x0001 muss der Assertion Consumer Service eine Tabelle verwalten, die Quell-IDs zu den Adressen der Partnerquellsites zuordnet.

4. **Das IVE sendet ein Authentication Statement an den ACS.**

   Das IVE verwendet das Statementhandle in der Anforderung, um das richtige Statement im IVE-Cache zu finden, und sendet dann das entsprechende Authentifizierungsstatement an den Assertion Consumer Service zurück. Das nicht signierte Statement enthält die Identität des Benutzers sowie den von ihm für die Anmeldung beim IVE verwendeten Mechanismus.

5. **Der ACS sendet ein Cookie an das IVE.**

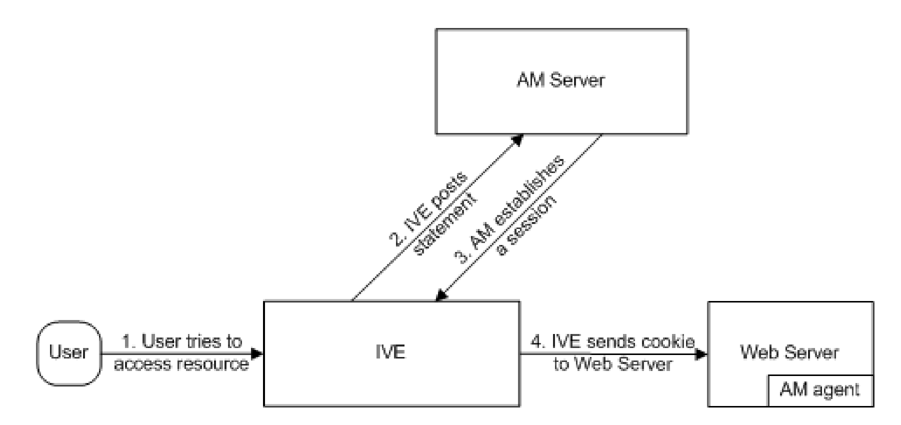
   Der Assertion Consumer Service akzeptiert das Statement und sendet dann ein Cookie an das IVE zurück, das die Benutzersitzung aktiviert.

6. **Das IVE sendet das Cookie an den Webserver.**

   Das Cookie wird vom IVE zwischengespeichert, um künftige Anforderungen verarbeiten zu können. Anschließend sendet das IVE das Cookie in einer HTTP-Anforderung an den Webserver, dessen Domänenname mit der Domäne im Cookie übereinstimmt. Der Webserver berücksichtigt die Sitzung, ohne den Benutzer zur Eingabe von Anmeldeinformationen aufzufordern.

POST-Profil

Wenn Sie sich für die Kommunikation mit einem ***POST-Profil*** (das auch als Browser/POST-Profil bezeichnet wird) entscheiden, leitet das IVE die Authentifizierungsdaten an das Zugriffsverwaltungssystem mithilfe eines HTTP POST-Befehls über eine SSL 3.0-Verbindung weiter. Dies wird im folgenden Diagramm dargestellt:



Das IVE und ein Zugriffsverwaltungssystem (Access Management, AM) gehen beim Weiterleiten von Informationen folgendermaßen vor:

1. **Der Benutzer möchte auf eine Ressource zugreifen.**

   Ein Benutzer ist beim IVE angemeldet und versucht, auf eine geschützte Ressource auf einem Webserver zuzugreifen.

2. **Das IVE stellt ein Statement bereit.**

   Das IVE fängt die Anforderung ab und überprüft, ob der erforderliche SSO-Vorgang bereits ausgeführt wurde, um die Anforderung zu berücksichtigen. Ist dies nicht der Fall, erstellt das IVE ein Authentifizierungsstatement, versieht es mit einer digitalen Signatur und stellt es direkt auf dem Zugriffsverwaltungsserver bereit. Da das Statement signiert ist, muss der Zugriffsverwaltungsserver der zum Ausstellen des Zertifikats verwendeten Zertifizierungsstelle vertrauen. Beachten Sie, dass Sie konfigurieren müssen, welches Zertifikat das IVE zum Signieren des Statements verwenden soll.

3. **Das AM stellt eine Sitzung her.**

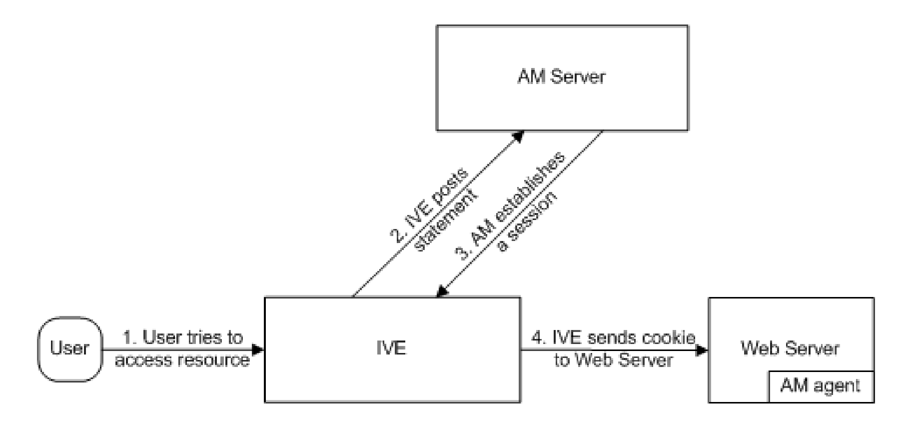
   Wenn der Benutzer über die entsprechenden Berechtigungen verfügt, sendet der Zugriffsverwaltungsserver ein Cookie an das IVE zurück, das die Benutzersitzung aktiviert.

4. **Das IVE sendet das Cookie an den Webserver.**

   Das Cookie wird vom IVE zwischengespeichert, um künftige Anforderungen verarbeiten zu können. Anschließend sendet das IVE das Cookie in einer HTTP-Anforderung an den Webserver, dessen Domänenname mit der Domäne im Cookie übereinstimmt. Der Webserver berücksichtigt die Sitzung, ohne den Benutzer zur Eingabe von Anmeldeinformationen aufzufordern.

Informationen zu Zugriffssteuerungsrichtlinien

Beim Aktivieren von Zugriffssteuerungstransaktionen für ein vertrauenswürdiges Zugriffsverwaltungssystem tauschen das IVE und das vertrauenswürdige Zugriffsverwaltungssystem Informationen mithilfe der im folgenden Diagramm dargestellten Methode aus:



Das IVE und ein Zugriffsverwaltungssystem (Access Management, AM) gehen beim Weiterleiten von Informationen folgendermaßen vor:

1. **Der Benutzer möchte auf eine Ressource zugreifen.**

   Ein Benutzer ist beim IVE angemeldet und versucht, auf eine geschützte Ressource auf einem Webserver zuzugreifen.

2. **Das IVE stellt eine Autorisierungsentscheidungsabfrage (Authorization Decision Query) bereit.**

   Wenn das IVE bereits eine Autorisierungsanforderung vorgenommen hat und diese noch gültig ist, verwendet das IVE diese Anforderung. (Die Gültigkeit der Autorisierungsanforderung ist in der IVE-Webkonsole festgelegt.) Wenn keine gültige Autorisierungsanforderung vorhanden ist, sendet das IVE eine Autorisierungsentscheidungsabfrage an das Zugriffsverwaltungssystem. Die Abfrage enthält die Identität des Benutzers sowie die Ressource, die das Zugriffsverwaltungssystem für die Autorisierung benötigt.

3. **Das AM sendet ein Authorization Decision Statement.**

   Das Zugriffsverwaltungssystem sendet einen HTTPS POST-Befehl mit einer SOAP-Nachricht, die das Authorization Decision Statement enthält. Das Authorization Decision Statement enthält eine Zusage, eine Verweigerung oder ein unbestimmtes Ergebnis.

4. **Das IVE sendet die Anforderung an den Webbrowser.**

   Wenn das Authorization Decision Statement eine Zusage zurückgibt, gewährt das IVE dem Benutzer den Zugriff. Andernfalls zeigt das IVE eine Fehlerseite an, auf der dem Benutzer mitgeteilt wird, dass er nicht über die entsprechenden Zugriffsberechtigungen verfügt.

Herstellen einer Vertrauensstellung zwischen SAML-fähigen Systemen

Damit Sie sicherstellen können, dass SAML-fähige Systeme Informationen nur zwischen vertrauenswürdigen Quellen weiterleiten, müssen Sie eine Vertrauensstellung zwischen den Anwendungen herstellen, die Informationen senden und empfangen. Zum Herstellen einer Vertrauens-stellung zwischen dem IVE und einer anderen SAML-fähigen Anwendung müssen Sie auf jedem System die folgenden Datentypen konfigurieren:

Vertrauenswürdige Anwendungs-URLs

Sie müssen bei einer Vertrauensstellung die URLs für die SAML-fähigen Systeme bereitstellen, die für die Kommunikation zwischen den Systemen erforderlich sind. Bei einigen Transaktionen muss nur das die Transaktion initiierende System (das IVE) den URL des anderen Systems kennen. (Das IVE verwendet den URL zum Initiieren der Transaktion.) Bei anderen Transaktionen (SSO-Transaktionen mit Artifact-Profilen) müssen Sie jedes System mit dem URL des anderen Systems konfigurieren.

Im Folgenden werden die verschiedenen Transaktionstypen und die jeweils zu konfigurierenden URLs aufgelistet:

- **SSO-Transaktionen: Artifact-Profil**

  Sie müssen auf dem IVE den URL des Assertion Consumer Service eingeben. Beispiel: `https://hostname/acs`

  Außerdem müssen Sie den folgenden URL für das IVE auf dem Assertion Consumer Service eingeben: `https://<IVEhostname>/dana-ws/saml.ws`

- **SSO-Transaktionen: POST-Profil**

  Sie müssen auf dem IVE den URL des Assertion Consumer Service eingeben. Beispiel: `https://hostname/acs`

- **Zugriffssteuerungstransaktionen**

  Sie müssen auf dem IVE den URL des SAML-Webdienstes eingeben. Beispiel: `https://hostname/ws`

Aussteller

Bevor ein Statement eines anderen Systems akzeptiert wird, muss eine SAML-fähige Einheit dem Aussteller des Statements vertrauen. Sie können steuern, welchen Ausstellern ein System vertraut, indem Sie bei der Systemkonfiguration die eindeutigen Zeichenfolgen der vertrauenswürdigen Aussteller angeben. (Beim Senden eines Statements identifiziert sich ein Aussteller durch Angeben seiner eindeutigen Zeichenfolge im Statement. SAML-fähige Anwendungen verwenden im Allgemeinen Hostnamen, um Aussteller zu identifizieren, der SAML-Standard lässt jedoch beliebige Zeichenfolgen für Anwendungen zu.) Wenn Sie ein System nicht für die Erkennung der eindeutigen Zeichenfolge eines Ausstellers konfigurieren, lässt das System keine Statements dieses Ausstellers zu.

Im Folgenden werden die verschiedenen Transaktionstypen und die zu konfigurierenden Aussteller aufgelistet:

- **SSO-Transaktionen**

  Sie müssen eine eindeutige Zeichenfolge auf dem IVE (in der Regel den jeweiligen Hostnamen) angeben, die das IVE verwenden kann, um sich zu identifizieren. Anschließend müssen Sie das Zugriffsverwaltungssystem für die Erkennung dieser Zeichenfolge konfigurieren.

- **Zugriffssteuerungstransaktionen**

  Sie müssen eine eindeutige Zeichenfolge auf dem Zugriffsverwaltungssystem (in der Regel den jeweiligen Hostnamen) angeben, die es verwenden kann, um sich zu identifizieren. Anschließend müssen Sie das IVE für die Erkennung dieser Zeichenfolge konfigurieren.

Zertifikate

Im Rahmen von SSL-Transaktionen muss der Server dem Client ein Zertifikat vorlegen, und anschließend muss der Client vor dem Akzeptieren der Informationen (zumindest) prüfen, ob er der Zertifizierungsstelle vertraut, die das Zertifikat des Servers ausgestellt hat. Sie können alle SAML-Transaktionen des IVE für die Verwendung von SSL (HTTPS) konfigurieren. In den folgenden Abschnitten werden die verschiedenen Transaktionstypen und die jeweiligen Zertifikatanforderungen aufgelistet.

SSO-Transaktionen: Artifact-Profil

Artifact-Profiltransaktionen beinhalten zahlreiche Kommunikationsvorgänge zwischen dem IVE und dem Zugriffsverwaltungssystem. Die von Ihnen zum Weiterleiten von Daten und zum Authentifizieren der beiden Systeme verwendeten Methoden haben Einfluss auf die zu installierenden und zu konfigurierenden Zertifikate. Im Folgenden werden die verschiedenen Konfigurationsoptionen für Artifact-Profile aufgelistet, für die besondere Zertifikatkonfigurationen erforderlich sind:

- **Alle Artifact-Profiltransaktionen**

  Unabhängig von der jeweiligen Konfiguration des Artifact-Profils müssen Sie das Zertifikat der Zertifizierungsstelle installieren, die das Zertifikat des IVE-Webservers auf dem Zugriffsverwaltungssystem signiert hat. (Für das IVE ist es erforderlich, dass das Zugriffsverwaltungssystem beim Anfordern eines Authentifizierungsstatements eine SSL-Verbindung verwendet. Bei einer SSL-Verbindung muss der Initiator dem System vertrauen, mit dem er eine Verbindung herstellt. Durch Installieren des Zertifizierungsstellenzertifikats auf dem Zugriffsverwaltungssystem stellen Sie sicher, dass das Zugriffsverwaltungssystem der Zertifizierungsstelle vertraut, die das IVE-Zertifikat ausgestellt hat.)

- **Senden von Artifacts über eine SSL-Verbindung (HTTPS GET-Anforderungen)**

  Wenn Sie Artifacts über eine SSL-Verbindung an das Zugriffsverwaltungssystem senden möchten, müssen Sie das Stammzertifizierungsstellen-Zertifikat des Zugriffsverwaltungssystems auf dem IVE installieren. (Bei einer SSL-Verbindung muss der Initiator dem System vertrauen, mit dem er eine Verbindung herstellt. Durch Installieren des Zertifizierungsstellenzertifikats des Zugriffsverwaltungs-systems auf dem IVE stellen Sie sicher, dass das IVE der Zertifizierungs-stelle vertraut, die das Zertifikat des Zugriffsverwaltungs-systems ausgestellt hat.) Sie können die Stammzertifizierungsstelle in der Webkonsole über die Seite **System > Configuration > Certificates > CA Certificates** installieren (Seite 190). Wenn Sie keine Artifacts über eine SSL-Verbindung senden möchten, müssen Sie keine zusätzlichen Zertifikate installieren.

  Wenn Sie SSL-basierte Kommunikationsverbindungen zwischen dem IVE und dem Zugriffsverwaltungssystem ermöglichen möchten, müssen Sie während der IVE-Konfiguration im Feld **SAML Assertion Consumer Service URL** einen URL eingeben, der mit HTTPS beginnt. Möglicherweise müssen Sie SSL auch auf dem Zugriffsverwaltungssystem aktivieren.

- **Transaktionen mit Zertifikatauthentifizierung**

  Zum Authentifizieren des Zugriffsverwaltungssystems mithilfe eines Zertifikats müssen Sie folgendermaßen vorgehen:

  - Installieren Sie das Stammzertifizierungsstellen-Zertifikat des Zugriffsverwaltungssystems auf dem IVE. Sie können die Stammzertifizierungsstelle in der Webkonsole über die Seite **System > Configuration > Certificates > CA Certificates** installieren (Seite 190).
  - Geben Sie an, welche Zertifikatwerte das IVE zum Überprüfen des Zugriffsverwaltungssystems verwenden soll. Sie müssen Werte verwenden, die mit den im Zertifikat des Zugriffsverwaltungsservers enthaltenen Werten übereinstimmen.

  Wenn Sie das Zugriffsverwaltungssystem nicht authentifizieren bzw. die Authentifizierung über Benutzername und Kennwort verwenden möchten, müssen Sie keine zusätzlichen Zertifikate installieren.

SSO-Transaktionen: POST-Profil

Im Rahmen einer POST-Profiltransaktion sendet das IVE signierte Authentifizierungsstatements an das Zugriffsverwaltungssystem. Im Allgemeinen werden diese über eine SSL-Verbindung gesendet (empfohlene Vorgehensweise), aber bei einigen Konfigurationen kann das IVE Statements auch über eine HTTP-Standardverbindung senden. Im Folgenden werden die verschiedenen Konfigurationsoptionen für POST-Profile aufgelistet, für die besondere Zertifikatkonfigurationen erforderlich sind:

- **Alle POST-Profiltransaktionen**

  Unabhängig von der jeweiligen Konfiguration des POST-Profils müssen Sie angeben, welches Zertifikat das IVE zum Signieren der zugehörigen Statements verwenden soll. Sie können ein Zertifikat in der Webkonsole auf der Seite **Resource Policies > Web > SAML > SSO > [Richtlinie] > General** auswählen (Seite 464). Anschließend müssen Sie das IVE-Zertifikat auf dem Zugriffsverwaltungssystem installieren. Sie können das IVE-Zertifikat von der Seite **System > Configuration > Certificates > Server Certificates > [Zertifikat] > Certificate Details** herunterladen (Seite 179).

- **Senden von POST-Daten über eine SSL-Verbindung (HTTPS)**

  Wenn Sie Statements über eine SSL-Verbindung an das Zugriffsverwaltungssystem senden möchten, müssen Sie das Stammzertifizierungsstellen-Zertifikat des Zugriffsverwaltungssystems auf dem IVE installieren. (Bei einer SSL-Verbindung muss der Initiator dem System vertrauen, mit dem er eine Verbindung herstellt. Durch Installieren des Zertifikats des Zugriffsverwaltungssystems auf dem IVE stellen Sie sicher, dass das IVE der Zertifizierungsstelle vertraut, die das Zertifikat des Zugriffsverwaltungssystems ausgestellt hat.) Sie können die

Stammzertifizierungsstelle in der Webkonsole über die Seite **System > Configuration > Certificates > CA Certificates** installieren (Seite 190). Wenn Sie keine Statements über eine SSL-Verbindung bereitstellen möchten, müssen Sie keine zusätzlichen Zertifikate installieren.

Wenn Sie SSL-basierte Kommunikationsverbindungen zwischen dem IVE und dem Zugriffsverwaltungssystem ermöglichen möchten, müssen Sie während der IVE-Konfiguration im Feld **SAML Assertion Consumer Service URL** einen URL eingeben, der mit HTTPS beginnt. Möglicherweise müssen Sie SSL auch auf dem Zugriffsverwaltungssystem aktivieren.

Zugriffssteuerungstransaktionen

Bei einer Zugriffssteuerungstransaktion sendet das IVE eine Autorisierungsentscheidungsabfrage an das Zugriffsverwaltungssystem. Sie müssen die für die Konfiguration erforderlichen Zertifikatoptionen ermitteln, um sicherzustellen, dass das Zugriffsverwaltungssystem auf die Abfrage reagiert. Im Folgenden werden die verschiedenen Konfigurationsoptionen für Zugriffssteuerungen aufgelistet, für die besondere Zertifikatkonfigurationen erforderlich sind:

- **Senden von Autorisierungsdaten über eine SSL-Verbindung**

  Wenn Sie mittels SSL eine Verbindung mit dem Zugriffsverwaltungssystem herstellen möchten, müssen Sie die Stammzertifizierungsstelle des Zugriffsverwaltungssystems auf dem IVE installieren. (Bei einer SSL-Verbindung muss der Initiator dem System vertrauen, mit dem er eine Verbindung herstellt. Durch Installieren des Zertifikats des Zugriffsverwaltungssystems auf dem IVE stellen Sie sicher, dass das IVE der Zertifizierungsstelle vertraut, die das Zertifikat des Zugriffsverwaltungssystems ausgestellt hat.) Sie können die Stammzertifizierungsstelle in der Webkonsole über die Seite **System > Configuration > Certificates > CA Certificates** installieren (Seite 190).

- **Transaktionen mit Zertifikatauthentifizierung**

  Wenn Sie die Zertifikatauthentifizierung verwenden möchten, müssen Sie das Zugriffsverwaltungssystem so konfigurieren, dass es der Zertifizierungsstelle vertraut, die das IVE-Zertifikat ausgestellt hat. Optional können Sie auch festlegen, dass das Zertifikat auf Grundlage der folgenden zusätzlichen Optionen akzeptiert wird:

  - Laden Sie den öffentlichen Schlüssel des IVE-Zertifikats auf das Zugriffsverwaltungssystem hoch.
  - Überprüfen Sie das IVE mithilfe bestimmter Zertifikatattribute.

  Diese Optionen erfordern die Angabe, welches Zertifikat das IVE an das Zugriffsverwaltungssystem weiterleiten soll. Sie können ein Zertifikat in der Webkonsole auf der Seite **Resource Policies > Web > SAML > Access Control > [Richtlinie] > General** wählen (Seite 470).

Informationen zum Konfigurieren des Zugriffsverwaltungssystems für die Überprüfung des IVE-Zertifikats finden Sie in der Dokumentation des Zugriffsverwaltungssystems. Wenn das Zugriffsverwaltungssystem keine Zertifikatauthentifizierung erfordert oder die Authentifizierung über Benutzername und Kennwort verwendet, müssen Sie das IVE nicht für die Weiterleitung eines Zertifikats an den Zugriffsverwaltungsserver konfigurieren. Wenn Sie keine Methode für Vertrauensstellungen festlegen, kann das Zugriffsverwaltungssystem Autorisierungs-anforderungen von jedem System akzeptieren.

Benutzeridentität

Im Rahmen einer Vertrauensstellung müssen die zwei Einheiten eine Methode der Identifizierung von Benutzern festlegen. Sie können einen Benutzernamen oder ein LDAP- oder ein Zertifikatbenutzerattribut für die gemeinsame Verwendung in den Systemen auswählen oder eine feste Benutzer-ID angeben. (Sie können beispielsweise das Feld **Subject Name** auf „Guest“ festlegen, um einen problemlosen Zugriff auf die Systeme zu ermöglichen.)

Damit Sie sicherstellen können, dass die zwei Systeme gemeinsame Informationen zu Benutzern weiterleiten, müssen Sie mithilfe der Optionen in der **Webkonsole** auf der Seite **Resource Policies > Web > SAML > SSO > [Richtlinie] > General** (Seite 464) und auf der Seite **Resource Policies > Web > SAML > Access Control > [Richtlinie] > General** (Seite 470) im Abschnitt **User Identity** festlegen, welche Informationen das IVE weiterleiten soll. Wählen Sie einen Benutzernamen oder ein Attribut aus, den bzw. das das Zugriffsverwaltungssystem erkennt.

Teil 3
IVE-Konfiguration

In diesem Abschnitt finden Sie Informationen zur Konfiguration und Verwaltung von Access Series-Produkten.

Inhalt

Konfigurieren der Seite „Status“

Die Seite **System > Status** enthält die folgenden Registerkarten:

Auf der Seite **System > Status** können Sie die folgenden Aufgaben durchführen:

Registerkarte „Overview“

Wenn Sie sich an der Webkonsole anmelden, ist die Seite **System > Status** ausgewählt, und die Registerkarte **Overview** wird angezeigt. Auf dieser Registerkarte sind die Details zum IVE-Server und den Systembenutzern zusammengefasst. Wenn Sie auf anderen Seiten der Webkonsole Änderungen vornehmen, werden die entsprechenden Informationen auf der Seite **General** aktualisiert.

Hinweis: Diese Registerkarte ist die Startseite für alle Administratoren, d. h. auch für Administratoren mit delegierten Rechten ohne Lese- oder Schreibzugriff auf die Registerkarten unter **System > Status**.

Auf dieser Seite können Sie Folgendes ausführen:

☑ Anzeigen der Auslastung der Systemkapazität

Das Central Manager-Dashboard für Access Series- und Meeting Series-Appliances bietet Diagramme über die Auslastung der Systemkapazität, in denen Sie problemlos ablesen und übersehen können, wie hoch die Systemauslastung normalerweise ist. Um diese Informationen an anderen Stellen für Datenberichte zu verwenden, können Sie sie anhand der Optionen auf der Seite **Maintenance > Import/Export > Configuration** als XML-Datei exportieren.

Diese Diagramme werden in der geöffneten Webkonsole auf der Registerkarte **System > Status > Overview** angezeigt, und Sie können Folgendes leicht ablesen:

- **Concurrent Users**

  Dieses Diagramm zeigt die Anzahl von Benutzern an, die am IVE angemeldet sind. Bei einer Cluster-Umgebung werden im Diagramm zwei Linien angezeigt. Die erste Linie zeigt die Anzahl der lokalen Benutzer an, die an dem Knoten angemeldet sind, der in der Dropdownliste ausgewählt ist, und die zweite Linie zeigt die Anzahl der gleichzeitig am gesamten Cluster angemeldeten Benutzer an.

- **Concurrent Meetings (nur Secure Meeting-Appliance)**

  Dieses Diagramm zeigt die Anzahl der gegenwärtig stattfindenden Konferenzen an. Bei einer Cluster-Umgebung werden im Diagramm zwei Linien angezeigt. Die erste Linie zeigt die Anzahl der Konferenzen an, die auf dem Knoten stattfinden, der in der Dropdownliste ausgewählt ist, und die zweite Linie zeigt die Anzahl der gleichzeitig im gesamten Cluster stattfindenden Konferenzen an.

- **Hits Per Second**

  Dieses Diagramm zeigt die Anzahl der gegenwärtig vom IVE verarbeiteten Zugriffe an. In einer Clusterumgebung legen Sie durch die Auswahl eines IVE aus der Dropdownliste den Knoten fest, dessen Daten im Diagramm angezeigt werden. Das Diagramm enthält vier Linien: Anzahl der Zugriffe, Anzahl der Webzugriffe, Anzahl der Dateizugriffe und Anzahl der Client/Server-Zugriffe.

- **CPU and Virtual (Swap) Memory Utilization**

  Dieses Diagramm zeigt den Prozentsatz der aktuellen CPU- und Speicherauslastung an. In einer Clusterumgebung legen Sie durch die Auswahl eines IVE aus der Dropdownliste den Knoten fest, dessen Daten im Diagramm angezeigt werden.

- **Throughput**

  Dieses Diagramm zeigt die gegenwärtig verarbeitete Datenmenge (in KB) an. In einer Clusterumgebung legen Sie durch die Auswahl eines IVE aus der Dropdownliste den Knoten fest, dessen Daten im Diagramm angezeigt werden. Das Diagramm enthält vier Linien: extern ein, extern aus, intern ein und intern aus.

Im Fenster **Page Settings** können Sie festlegen, welche Diagramme das IVE im Dashboard anzeigt und für welchen Zeitraum das IVE die Daten verfolgt.



Abbildung 12: Seite „System > Status > Overview“

☑ XML-Daten aus Diagrammen herunterladen

So laden Sie Diagrammdaten in eine XML-Datei herunter:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf die Verknüpfung **Edit**, die dem Diagramm entspricht, das Sie herunterladen möchten.
3. Geben Sie das Verzeichnis an, in dem Sie die XML-Datei speichern möchten, und klicken Sie auf **Save**.

☑ Angeben des Zeitraums und der Daten, die in Diagrammen dargestellt werden sollen

So geben Sie den Zeitraum und die Daten an, die in Diagrammen dargestellt werden sollen:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf **Page Settings**.
3. Wählen Sie aus, welche Auslastungsdiagramme angezeigt werden sollen.
4. Wählen Sie den Zeitraum aus, der in den Diagrammen dargestellt werden soll. Die Intervalle können zwischen 1 Stunde und 1 Jahr liegen.
5. Geben Sie an, wie oft die Diagramme aktualisiert werden sollen.
6. Klicken Sie auf **Save Changes**.

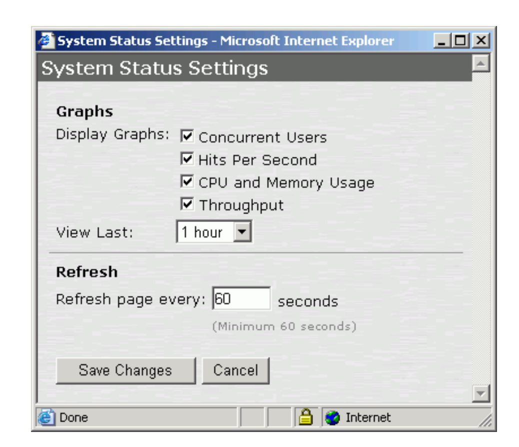


Abbildung 13: **Seite „System > Status > Overview > Page Settings“**

☑ Konfigurieren der Diagrammanzeige

So geben Sie die in Diagrammen angezeigten Farben und die Linienstärke an:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf die Verknüpfung **Edit**, die dem Diagramm entspricht, das Sie ändern möchten.
3. Verwenden Sie die Einstellungen im Dialogfeld **Graph Settings** zur Bearbeitung von Hintergrundfarbe, Diagrammlinienfarben, Textfarbe, Linienfarbe und Linienstärke des Diagramms.
4. Klicken Sie auf **Save Changes**.

☑ Anzeigen kritischer Systemereignisse

Mit dem Central Manager-Dashboard für Access Series- und Meeting Series-Appliances können Sie ganz einfach die letzten zehn kritischen Systemereignisse anzeigen. Im Fenster **Event Monitor** können Sie schnell auf kritische Systemprobleme zugreifen und diese behandeln. Während Sie in der Webkonsole Routineaufgaben zur Wartung und Konfiguration ausführen, können Sie das Fenster **Event Monitor** geöffnet lassen und die Systemereignisse überwachen.

So zeigen Sie schnell kritische Systemereignisse an:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf **Critical Events**. Im Fenster **Event Monitor** werden der Schweregrad und eine Meldung zu kritischen Ereignissen in der Systemprotokolldatei angezeigt.
3. Klicken Sie auf **Refresh**, um die neuesten Ereignisse anzuzeigen (optional).
4. Klicken Sie auf **See All**, um zur Registerkarte **System > Log/Monitoring > Events > Log** zu navigieren, auf der alle Ereignisse, von informativ bis kritisch, angezeigt werden (optional). Weitere Informationen finden Sie unter „Konfigurieren der Seite „Log Monitoring““ auf Seite 249.

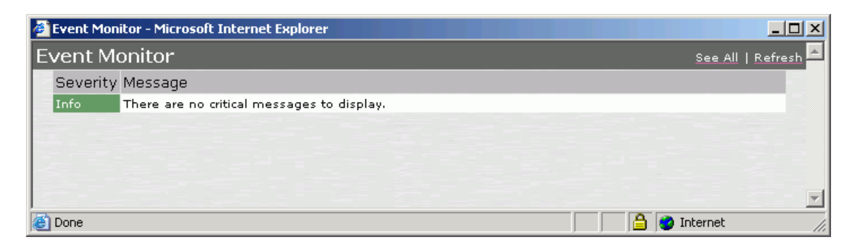


Abbildung 14: **Seite „System > Status > Overview > Critical Events“**

☑ Herunterladen des aktuellen Servicepakets

Auf der Registerkarte **System > Status > Overview** können Sie das Servicepaket herunterladen, dass zurzeit im IVE installiert ist, damit Sie es leicht speichern und auf einem anderen IVE installieren können.

So laden Sie das aktuelle Servicepaket herunter:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf **Download Package** (Central Manager-Version) oder auf die Verknüpfung neben **System Software Pkg Version**.
3. Klicken Sie auf **Speichern**.
4. Geben Sie einen Namen und einen Speicherort für das Servicepaket an.
5. Klicken Sie auf **Speichern**.

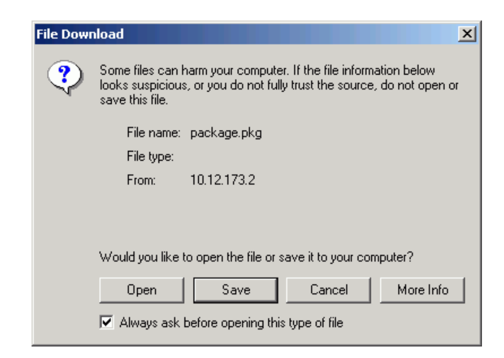


Abbildung 15: **Seite „System > Status > Overview > Download Package“**

☑ Bearbeiten von Systemdatum und -zeit

Sie müssen die Serverzeit einstellen, damit die Systemereignisse und die Übertragung von Benutzerdateien genau aufgezeichnet werden. Sie können das IVE über einen NTP-Server (Network Time Protocol) mit anderen Computern synchronisieren oder die IVE-Zeit manuell einrichten.

So bearbeiten Sie Systemdatum und -zeit:

1. Wählen Sie in der Webkonsole **System > Status > Overview** aus.
2. Klicken Sie im Abschnitt **System Date & Time** auf **Edit**.
3. Wählen Sie im Menü **Time Zone** eine Zeitzone aus. Das IVE passt die Uhrzeit automatisch an die Sommerzeit an.
4. Stellen Sie die Systemzeit mithilfe einer der folgenden Methoden ein:
   - **Use NTP server**

     Wählen Sie die Option **Use NTP Server** aus, geben Sie die IP-Adresse oder den Namen des Servers ein, und geben Sie ein Aktualisierungs-intervall an.
   - **Set Time Manually**

     Wählen Sie die Option **Set Time Manually** aus, und geben Sie Werte für Datum und Uhrzeit ein. Sie können auch auf **Get from Browser** klicken, damit Daten in die Felder **Date** und **Time** eingegeben werden.
5. Klicken Sie auf **Save Changes**.

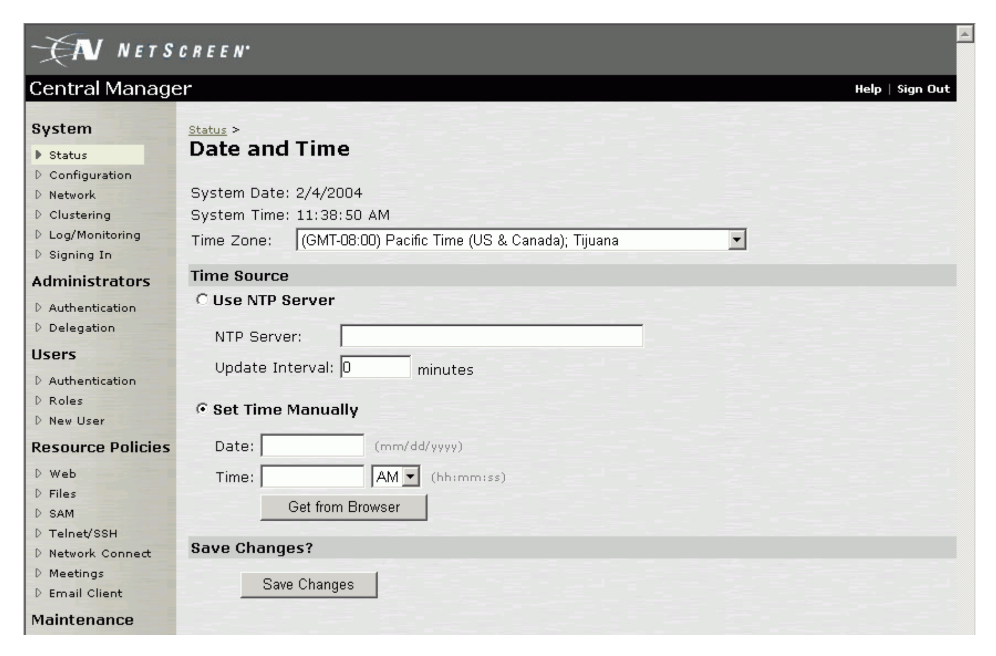


Abbildung 16: **System > Status > Overview > Date and Time**

Registerkarte „Active Users“

☑ Überwachen von Benutzern mit Anmeldung am IVE

Über das Menü **Active Users** können Sie Benutzer überwachen, die am IVE angemeldet sind. Dabei werden der Name jedes Benutzers, der Authentifizierungsbereich und die Anmeldezeit aufgeführt. Beachten Sie, dass Nicht-IVE-Benutzer, die an einem Secure Meeting angemeldet sind, als Mitglieder der Rolle „Secure Meeting User Role“ aufgeführt werden.

Hinweis: Das IVE zeigt für Nicht-IVE-Benutzer, die sich zur Teilnahme an einem Secure Meeting am IVE angemeldet haben, in den Spalten **Realm** und **Role** „N/A“ (keine Angabe) an.

So überwachen Sie am IVE angemeldete Benutzer:

1. Wählen Sie in der Webkonsole **System > Status > Active Users** aus.
2. Führen Sie bei Bedarf die folgenden Vorgänge durch:
   - **Abmelden von Benutzern von einer IVE-Sitzung:**
     - Um einen oder mehrere Endbenutzer oder Administratoren zwangsweise abzumelden, aktiveren Sie die Kontrollkästchen neben den entsprechenden Namen, und klicken Sie dann auf **Delete Session**.
     - Um alle aktuell angemeldeten Endbenutzer zwangsweise abzumelden, klicken Sie auf **Delete All Sessions**. (Beachten Sie, dass Sie Administratoren für die Abmeldung einzeln auswählen und die Schaltfläche **Delete Session** verwenden müssen.)
   - **Konfigurieren der angezeigten Daten und ihrer Reihenfolge:**
     - Geben Sie zum Anzeigen eines bestimmten Benutzers seinen Benutzernamen im Feld **Show Users Named** ein, und klicken Sie auf **Update**. Wenn Sie den genauen Benutzernamen nicht kennen, verwenden Sie einen Platzhalter (*). Wenn z. B. ein Benutzer „Joseph Jones" heißt, Sie sich aber nicht erinnern können, ob der Benutzername „Joe" oder „Joseph" lautet, geben Sie im Feld **Show Users Named** die Zeichenfolge „Jo*" ein Das IVE gibt eine Liste aller Benutzer zurück, deren Benutzername mit den Buchstaben „jo" beginnt.
     - Um zu steuern, wie viele Benutzer und Administratoren auf der Seite **Active Users** angezeigt werden, geben Sie im Feld **Show *N* users** eine Zahl ein, und klicken Sie auf **Update**.
     - Um die Tabelle der aktuell angemeldeten Benutzer und Administratoren zu sortieren, klicken Sie auf eine Spaltenüberschrift.
     - Klicken Sie zum Aktualisieren des Seiteninhalts auf **Update**.
   - **Erstellen einer Verknüpfung mit weiteren Registerkarten:**
     - Klicken Sie zum Bearbeiten des Authentifizierungsbereichs eines Benutzers neben dem Namen auf die Verknüpfung **Realm**, und folgen Sie den Anweisungen unter „Konfigurieren eines Authentifizierungsbereichs" auf Seite 379.
     - Klicken Sie zum Bearbeiten der Rolle eines Benutzers auf die Verknüpfung **Role** neben seinem Namen, und folgen Sie den Anweisungen unter „Konfigurieren der Seite „Delegation"" auf Seite 355 (für Administratoren) oder „Konfigurieren der Seite „Roles"" auf Seite 393 (für Endbenutzer).

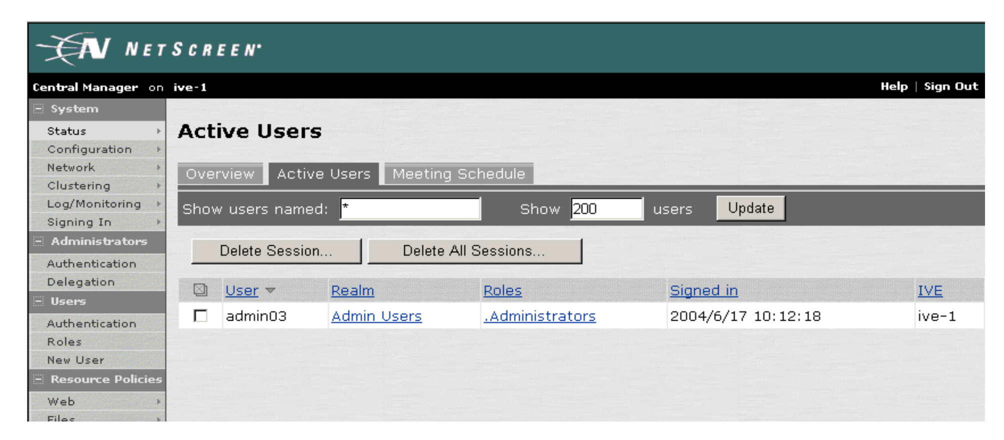


Abbildung 17: **System > Status > Active Users**

Registerkarte „Meeting Schedule"

☑ Anzeigen und Absagen geplanter Konferenzen

Zeigen Sie mit den Seiten **Meeting Schedule** (Access Series-Appliance) oder **Schedule** (Meeting Series-Appliance) alle gegenwärtig auf dem IVE geplanten Konferenzen an, und sagen Sie ggf. Konferenzen ab. (Eine Beschreibung der Option „Secure Meeting" finden Sie unter „Secure Meeting – Übersicht" auf Seite 15.)

So zeigen Sie geplante Konferenzen an oder sagen diese ab:

1. Wählen Sie in der Webkonsole **System > Status > Meeting Schedule** (Access Series-Appliance) oder **System > Schedule** (Meeting Series-Appliance) aus. Das IVE zeigt Echtzeitinformationen zu allen gegenwärtig ausgeführten oder geplanten Konferenzen an, einschließlich:

   - **Zeit und Status**

     Zeigt die geplante Zeit und Dauer der Konferenz sowie den aktuellen Status an.

   - **Konferenzdetails**

     Zeigt den Konferenznamen sowie ID- und Kennwortanforderungen an. Diese Spalte enthält außerdem eine Verknüpfung **Details**, über die Sie Informationen zur Konferenz und Konferenzteilnahme anzeigen können.

- **Meeting Role**

  Zeigt die Rolle des Konferenzerstellers an. Wenn der Ersteller beim Erstellen der Konferenz unter mehreren Rollen angemeldet war (wenn er z. B. Mitglied mehrerer Rollen ist und die Appliance für eine permissive Zusammenführung konfiguriert ist), wählt Secure Meeting eine Rolle aus, wie unter „Registerkarte „Meetings““ auf Seite 433 dargestellt.

- **Attendee Roles**

  Zeigt die Rollen der für die Konferenz angemeldeten Teilnehmer, die Anzahl der für jede Rolle angemeldeten Teilnehmer und die Teilnehmerobergrenze für jede Rolle an. Beachten Sie, dass Nicht-IVE-Teilnehmer unter der Benutzerrolle des Konferenzleiters aufgeführt werden. Informationen darüber, wie Teilnehmer zu Rollen zugewiesen und wie Obergrenzen für eine Rolle festgelegt werden, finden Sie unter „Aktivieren und Konfigurieren von Konferenzen für Benutzerrollen“ auf Seite 433.

2. Mithilfe der folgenden Methoden können Sie die Konferenzansicht ändern (optional):
   - Wählen Sie aus den Gruppenregisterkarten (Meeting Series-Appliance) oder in der Dropdownliste (Access Series-Appliance) einen Zeitrahmen aus (**Daily**, **Weekly**, **In Progress** oder **Scheduled**), um festzulegen, welche Konferenzen angezeigt werden.
   - Klicken Sie auf eine beliebige unterstrichene Spaltenüberschrift, um die Sortierreihenfolge der derzeit angezeigten Konferenzen zu steuern.
3. Klicken Sie unterhalb einer Konferenz auf die Verknüpfung **Details**, um Informationen zur Konferenz anzuzeigen und dieser ggf. beizutreten (optional).
4. Klicken Sie auf das Löschsymbol in der rechten Spalte, um eine Konferenz abzusagen (optional).

Wichtig: Durch das Absagen wird eine Konferenz endgültig aus dem IVE gelöscht. Sie können eine Konferenz nach dem Absagen nicht wiederherstellen.

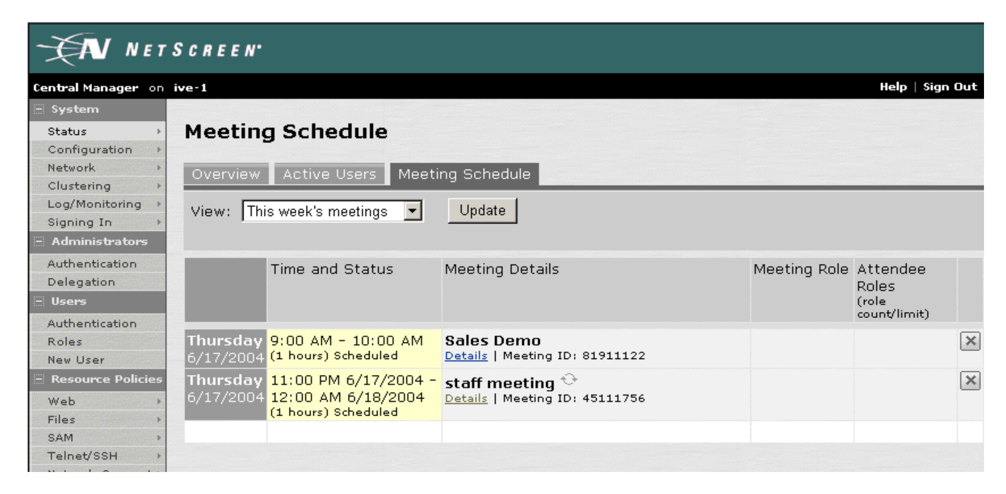


Abbildung 18: **System > Status > Meeting Schedule**

Konfigurieren der Seite „Schedule“

Auf der Seite **Schedule** (Meeting Series-Appliance) können Sie alle gegenwärtig auf dem IVE geplanten Konferenzen anzeigen und Konferenzen ggf. absagen. Weitere Informationen finden Sie unter „Registerkarte „Meeting Schedule““ auf Seite 157.

Konfigurieren der Seite „Configuration“

Die Seite **System > Configuration** enthält die folgenden Registerkarten:

Auf der Seite **System > Configuration** können Sie die folgenden Aufgaben durchführen:

Registerkarte „Licensing“

Das IVE enthält eine Lizenz für den Standardzugriff auf das IVE[1]. Um das System im vollen Umfang nutzen zu können, müssen Sie sich jedoch an der Webkonsole anmelden und die Lizenzen eingeben, die Sie per E-Mail von Juniper Networks erhalten haben. Die E-Mail kann bis zu drei unterschiedliche Arten von Lizenzen enthalten:

- **Produktlizenz** – Eine ***Produktlizenz*** bestimmt die Anzahl von IVEs in einem Cluster sowie die Anzahl von Benutzern, die sich gleichzeitig beim System anmelden können. Ihre Produktlizenz kann z. B. erlauben, dass Sie einen 4-Unit-Cluster aus A5000-Einheiten mit 2.500 Benutzern erstellen, die gleichzeitig zugreifen können.
- **Lizenz für Aktualisierungspakete** – Mit einer ***Lizenz für Aktualisierungspakete*** können Sie eine Reihe von Funktionen verwenden. Wenn Sie über eine Central Manager-Lizenz verfügen, können Sie verschiedene Funktionen verwenden: IVE-Dashboard-Funktion zum Überwachen der Systemkapazität, Konfigurationsübertragungsfunktion zum Übernehmen der Einstellungen aus einem IVE in ein anderes, Funktion für ausfallfreie Aktualisierungen zum Beschleunigen von Aktualisierungen, Sicherungsfunktion zum lokalen Speichern von Sicherungsdateien und Protokollberichtsfunktion zum Anpassen des Protokolldateiformats.
- **Lizenz für die Aktualisierungsfunktion** – Mit einer ***Lizenz für die Aktualisierungsfunktion*** können Sie eine einzelne Funktion verwenden. Mit einer Secure Terminal-Lizenz können Sie z. B. von jedem Benutzercomputer aus über Telnet oder SSH auf gehostete Server sicher zugreifen.

Geben Sie mithilfe der Registerkarte **System > Configuration > Licensing** die Lizenzcodes für Ihre Site ein, zeigen Sie die Ablaufdaten ein, und löschen Sie diese ggf.

Hinweis: Lesen Sie in jedem Fall die Lizenzvereinbarung, auf die Sie über die Registerkarte **Licensing** zugreifen können, bevor Sie Ihre Lizenz senden. Bei der über die Registerkarte **Licensing** verfügbaren Lizenzvereinbarung handelt es sich um denselben Text, der während des ersten Setups an der seriellen Konsole angezeigt wird.

---

1. Mit der grundlegenden IVE-Lizenz können Sie fünf lokale Benutzerkonten erstellen, zwei Benutzer können sich gleichzeitig anmelden, und es werden grundlegende Funktionen zum Navigieren durch Web-, Windows- und UNIX/NFS-Dateien bereitgestellt.

☑ Eingeben oder Aktualisieren einer IVE-Lizenz

So geben Sie die IVE-Lizenz ein oder aktualisieren diese:

1. Wählen Sie in der Webkonsole **System > Configuration > Licensing** aus.
2. Klicken Sie auf die Verknüpfung **License Agreement**. Lesen Sie die Lizenzvereinbarung. Wenn Sie mit den Bestimmungen einverstanden sind, fahren Sie mit dem nächsten Schritt fort.
3. Geben Sie den Firmennamen und den Lizenzschlüssel ein, und klicken Sie dann auf **Save changes**.

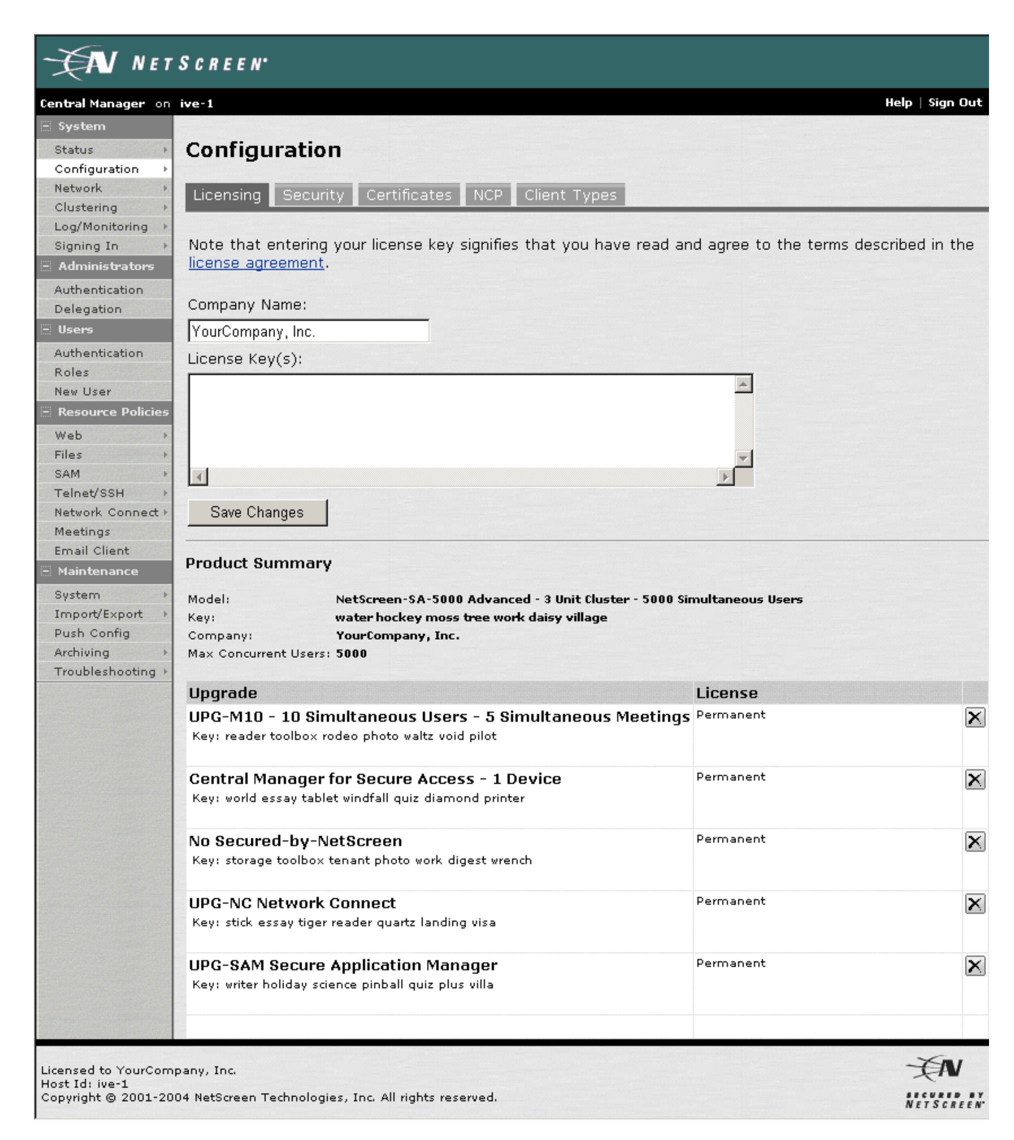


Abbildung 19: System > Configuration > Licensing

Registerkarte „Security > Security Options“

Mit der Registerkarte **System > Configuration > Security > Security Options** können Sie die Standardsicherheitseinstellungen für das IVE festlegen. Wir empfehlen, die Standardsicherheitseinstellungen zu verwenden, die höchste Sicherheit bereitstellen. Falls die Benutzer bestimmte Browser nicht verwenden oder auf bestimmte Webseiten nicht zugreifen können, müssen Sie diese Einstellungen jedoch möglicherweise ändern.

☑ Festlegen von systemweiten Sicherheitsoptionen

Wenn bei Benutzern beim Zugriff auf bestimmte Webseiten Browserprobleme auftreten, müssen Sie ggf. Folgendes anpassen:

- **Zulässige SSL- bzw. TLS-Version**

  Für den IVE sind standardmäßig SSL, Version 3, und TLS erforderlich. In älteren Browsern wird SSL, Version 2, verwendet. Sie können entweder die Benutzer ihre Browser aktualisieren lassen oder die Einstellung ändern, damit sowohl SSL, Version 2, als auch SSL, Version 3, zulässig sind.

- **Zulässige Verschlüsselungsstärke**

  Für den IVE ist standardmäßig 128-Bit-Verschlüsselung erforderlich. Sie können außerdem angeben, dass für das IVE 168-Bit-Verschlüsselung erforderlich ist. In älteren Browsern, die vor der Änderung des US-Exportgesetzes im Jahr 2000 entwickelt wurden, das bis dahin für den internationalen Export eine Verschlüsselungsstärke von 40 Bit vorschrieb, wird u. U. noch die 40-Bit-Verschlüsselung verwendet. Sie können entweder den Benutzern mitteilen, dass diese eine Aktualisierung auf einen Browser mit 128-Bit-Verschlüsselung vornehmen sollen, oder die erforderliche Verschlüsselungsstärke ändern, so dass auch die 40-Bit-Verschlüsselung zulässig ist.

  Hinweis: Bei Verwendung von 168-Bit-Verschlüsselung für das IVE zeigen manche Webbrowser möglicherweise immer noch 128-Bit-Verschlüsselung an (das goldene Schloss auf der Statusleiste des Browsers), auch wenn es sich um 168-Bit-Verbindung handelt. Dabei kann es sich um eine Funktionsbeschränkung des Browsers handeln.

- **Navigation zu SSL-Sites**

  Der IVE gestattet die Navigation zu internen SSL-Sites (denen https:// vorangestellt ist) und akzeptiert als Standard sämtliche (temporären oder anderen) Zertifikate. Falls Sie Bedenken wegen Benutzern haben, die über das IVE zu Sites ohne Zertifikate von einer gültigen externen Zertifizierungsstelle navigieren, deaktivieren Sie diese Funktion.

- **Vermittlung der Standardauthentifizierung**

  Das IVE kann die Anmeldeinformationen von Benutzern vermitteln, um zu verhindern, dass ein Benutzer über die zwischengespeicherten Anmeldeinformationen eines anderen Benutzers auf Ressourcen zugreifen kann. Darüber hinaus kann das IVE die Anmeldeinformationen von Benutzern wiederverwenden und ermöglicht somit die Einzelanmeldung (Single Sign-In) für andere Intranetsites. Wenn Sie die Option für die Einzelanmeldung auswählen, stellt das IVE sicher, dass die Anmeldeinformationen nur innerhalb des Firmenintranets weitergeleitet werden.

- **Löschen aller Cookies beim Abbruch der Sitzung**

  Aus praktischen Gründen legt das IVE auf dem Computer des Benutzers permanente Cookies fest, z. B. das Cookie für den letzten Bereich und das Cookie für die letzte Anmeldung. Wenn Sie mehr Sicherheit oder Datenschutz wünschen, können Sie das Festlegen dieser Cookies verhindern.

- **Einfügen des IVE-Sitzungscookies in URL**

  Mozilla 1.6 und Safari geben möglicherweise keine Cookies an die Java Virtual Machine weiter, wodurch verhindert wird, dass Benutzer JSAM und Java-Applets ausführen. Um diese Browser zu unterstützen, kann das IVE das Benutzersitzungscookie in den URL einfügen, der JSAM oder ein Java-Applet aufruft. Standardmäßig ist diese Option aktiviert. Wenn Sie aber Bedenken haben, das Cookie im URL verfügbar zu machen, können Sie diese Funktion deaktivieren.

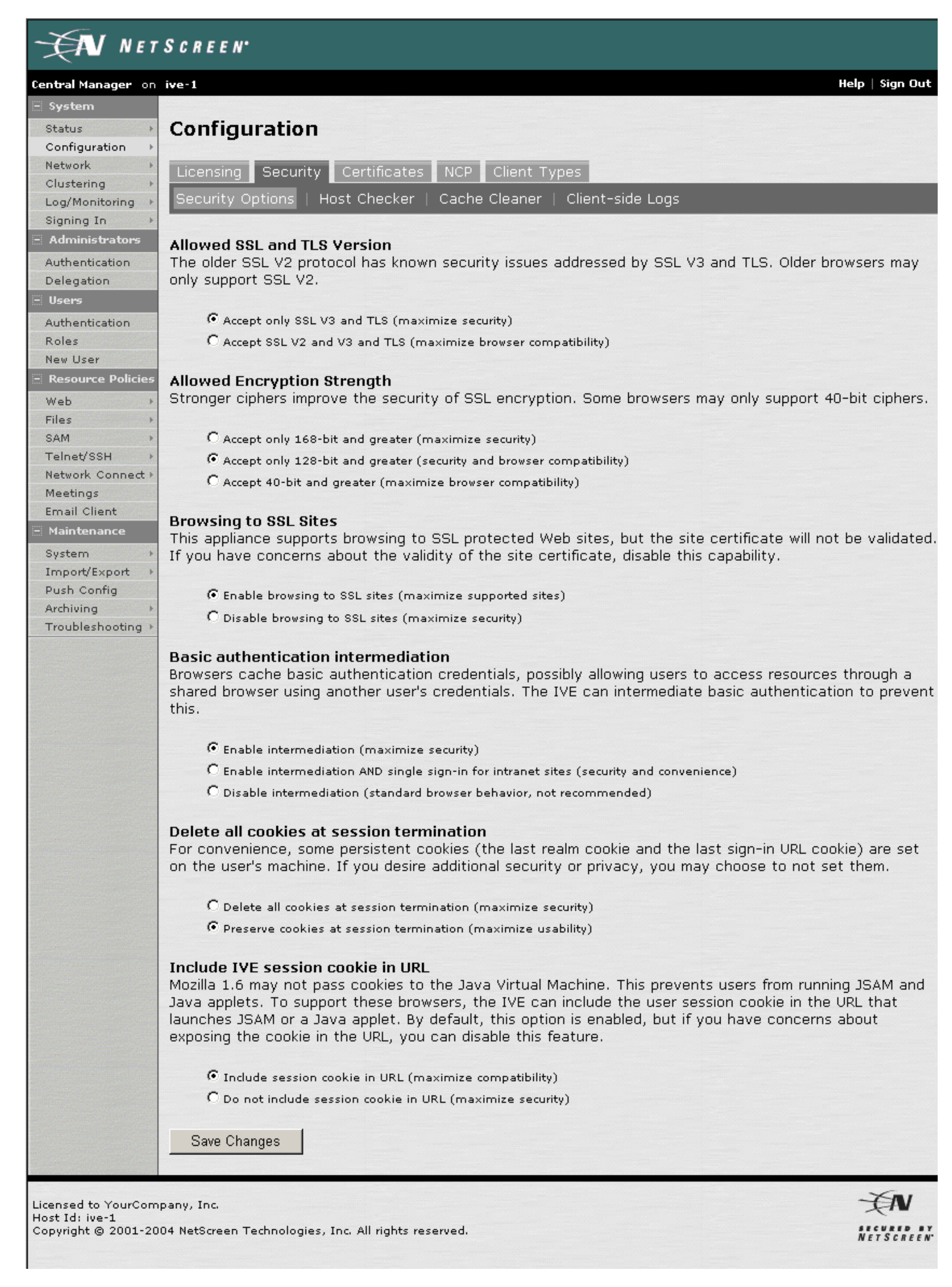


Abbildung 20: **System > Configuration > Security > Security Options**

Registerkarte „Security > Host Checker“

Auf der Registerkarte **System > Configuration > Security > Host Checker** (Hostprüfung) können Sie Folgendes ausführen:

☑ Angeben von Hostprüfung-Optionen

Sie können globale Optionen für die Hostprüfung angeben, die auf alle Benutzer angewendet werden können, für die in einer Authentifizierungsrichtlinie, einer Rollenzuordnungsregel oder einer Ressourcenrichtlinie die Hostprüfung erforderlich ist.

So geben Sie Optionen für die Hostprüfung an:

1. Wählen Sie in der Webkonsole **System > Configuration > Security > Host Checker** aus.
2. Geben Sie unter **Options** Folgendes an:
   - Das Intervall in Minuten, in dem die Hostprüfung auf einem Clientcomputer ausgeführt werden soll. Wenn der Clientcomputer die von einer Rolle oder Ressourcenrichtlinie gestellten Anforderungen der Richtlinien für die Hostprüfung nicht erfüllt, verweigert das IVE die entsprechenden Benutzeranfragen.

     Beispielsweise kann verlangt werden, dass ein Benutzer eine bestimmte Antivirenanwendung eines Drittanbieters ausführt, um Rolle A zugeordnet zu werden, wodurch Netzwerkverbindungen von einem externen Standort aktiviert werden. Wenn bei der Anmeldung des Benutzers beim IVE auf dem Clientcomputer des Benutzers die erforderliche Antivirenanwendung ausgeführt wird, wird der Benutzer Rolle A zugeordnet und erhält sämtliche zugehörigen Zugriffsmöglichkeiten. Wenn aber die Antivirenanwendung während der Benutzersitzung beendet wird, erfüllt der Benutzer bei der nächsten Ausführung der Hostprüfung die Sicherheitsanforderungen für Rolle A nicht mehr und verliert deshalb sämtliche Zugriffsberechtigungen für diese Rolle.

- Aktivieren Sie **Auto-upgrade Host Checker**, wenn das IVE die Hostprüfung automatisch auf einen Clientcomputer herunterladen soll, wenn die Version der Hostprüfung auf dem IVE neuer ist, als die auf dem Client installierte Version. Beachten Sie bei Auswahl dieser Option Folgendes:
  - Damit das IVE die Hostprüfung automatisch auf dem Client installiert, müssen Benutzer über Administratorberechtigungen verfügen.
  - Wenn ein Benutzer die Hostprüfung deinstalliert und sich dann an einem IVE anmeldet, für das die Option **Auto-upgrade Host Checker** nicht aktiviert ist, kann der Benutzer nicht länger auf die Hostprüfung zugreifen.

3. Klicken Sie auf **Save Changes**.

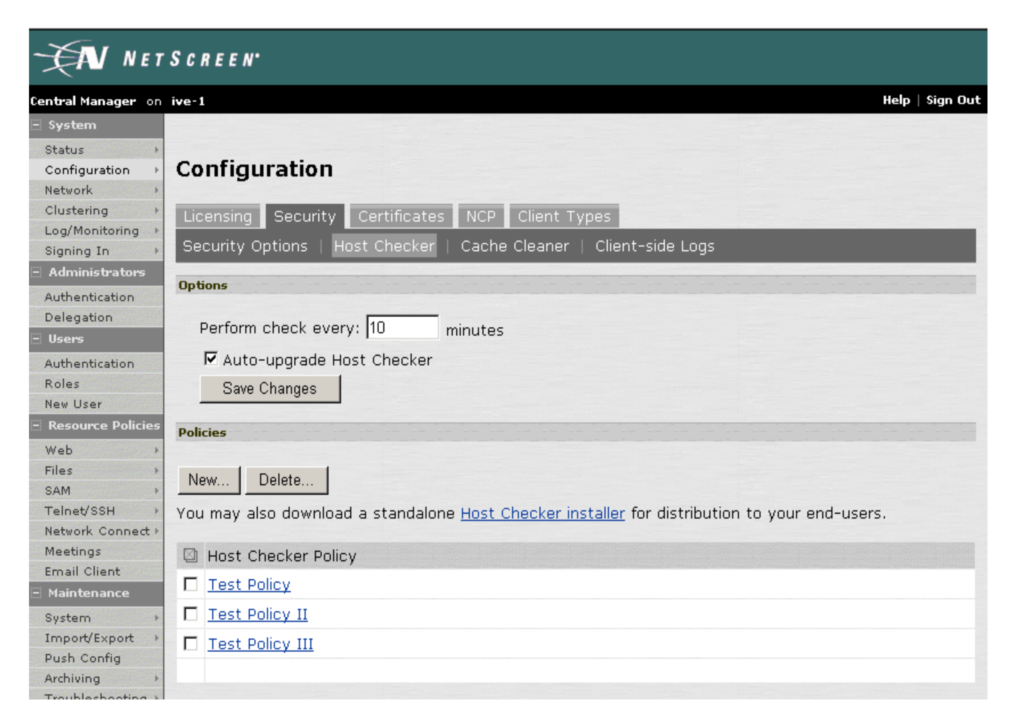


Abbildung 21: **System > Configuration > Security > Host Checker**

☑ Erstellen einer globalen Hostprüfung-Richtlinie

Sie müssen die Hostprüfung-Richtlinien erstellen, auf die Sie dann in Authentifizierungsrichtlinien (für Authentifizierungsbereiche), Rollenzuordnungsregeln und Ressourcenrichtlinien verweisen können. Weitere Informationen finden Sie unter „Hostprüfung – Übersicht“ auf Seite 99.

So erstellen Sie eine globale Hostprüfung-Richtlinie:

1. Wählen Sie in der Webkonsole **System > Configuration > Security > Host Checker** aus.
2. Klicken Sie unter **Policies** auf **New**.
3. Geben Sie auf der Seite **Configuration** im Feld **Policy Name** einen Namen ein, und klicken Sie dann auf **Continue**.
4. Wählen Sie unter **Host Checking Method** eine beliebige Anzahl der folgenden Optionen aus (optional):
   - **Sygate Enforcement API** – Zur Verwendung dieser Option muss das Produkt Sygate Personal Firewall auf dem Clientcomputer installiert sein.
   - **Sygate Security Agent** – Zur Verwendung dieser Option muss Sygate Security Agent auf dem Clientcomputer installiert sein.
   - **Zone Labs: Zone Alarm Pro and Zone Labs Integrity** – Zur Verwendung dieser Option muss entweder Zone Alarm Pro oder Zone Labs Integrity auf dem Clientcomputer installiert sein.
   - **McAfee Desktop Firewall 8.0** – Zur Verwendung dieser Option muss McAfee Desktop Firewall 8.0 auf dem Clientcomputer installiert sein.
   - **InfoExpress CyberGatekeeper Agent** – Zur Verwendung dieser Option muss das Produkt InfoExpress CyberGatekeeper Agent auf dem Clientcomputer installiert sein.
5. Wählen Sie unter **Rule Settings** in der Dropdownliste einen Regeltyp aus (Beschreibungen finden Sie auf Seite 100), und klicken Sie dann auf **Add** (optional). Das Konfigurationsdialogfeld für diese Regel wird angezeigt. Gehen Sie in den jeweiligen Konfigurationsdialogfeldern folgendermaßen vor:
   - **3rd Party NHC Integration**:
     1. Geben Sie den Namen für die DLL ein.
     2. Geben Sie den Speicherort der DLL auf den Clientcomputern (Pfad und Dateiname) an.
     3. Klicken Sie auf **Save Changes**.

- **Attribute Check: Ports**:
  1. Geben Sie eine Liste von Ports mit Kommas als Trennzeichen (ohne Leerzeichen) oder einen Bereich von Ports ein, beispielsweise: `1234,11000-11999,1235`.
  2. Wählen Sie **Required**, um zu bestimmen, dass diese Ports auf dem Clientcomputer geöffnet sein müssen, oder **Deny**, um zu bestimmen, dass sie geschlossen sein müssen.
  3. Klicken Sie auf **Save Changes**.
- **Attribute Check: Process**:
  1. Geben Sie den Namen eines Prozesses (ausführbare Datei) ein, beispielsweise: `good-app.exe`.
  2. Wählen Sie **Required** aus, um zu fordern, dass dieser Prozess im Task-Manager ausgeführt wird, oder wählen Sie **Deny** aus, um zu fordern, dass dieser Prozess nicht ausgeführt wird.
  3. Geben Sie den MD5-Prüfsummenwert für jede der ausführbaren Dateien ein, auf die die Richtlinie angewendet werden soll (optional). Beispielsweise kann eine ausführbare Datei auf einem Desktop, einem Laptop oder verschiedenen Windows-Betriebssystemversionen unterschiedliche MD5-Prüfsummenwerte aufweisen. Geben Sie alle gültigen Werte an.
  4. Klicken Sie auf **Save Changes**.
- **Attribute Check: File**:
  1. Geben Sie den Namen einer Datei (eines beliebigen Dateityps) ein, beispielsweise: `\Temp\Bad-file.doc`.
  2. Wählen Sie **Required** aus, um zu fordern, dass diese Datei auf dem Clientcomputer vorhanden ist, oder wählen Sie **Deny** aus, um zu fordern, dass diese Datei nicht vorhanden ist.
  3. Geben Sie das maximale Alter der Datei in Tagen an (optional). Wenn die Datei älter als die angegebene Anzahl von Tagen ist, entspricht der Client nicht den Anforderungen der Attributprüfung.

     Tipp:

     Mit dieser Option können Sie das Alter der Virensignaturen überprüfen. Geben Sie (im Feld **File Name**) den Pfad zu einer Datei an, deren Zeitstempel angibt, wann die Virensignaturen zuletzt aktualisiert wurden, z. B eine Virensignaturdatenbank oder Protokolldatei, die jedes Mal beim Aktualisieren der Datenbank ebenfalls aktualisiert wird. Wenn Sie beispielsweise TrendMicro verwenden, können Sie Folgendes angeben: `C:\Programme\Trend Micro\OfficeScan Client\TmUpdate.ini`.
  4. Geben Sie den MD5-Prüfsummenwert für jede der ausführbaren Dateien ein, auf die die Richtlinie angewendet werden soll (optional).
  5. Klicken Sie auf **Save Changes**.

- **Attribute Check: Registry Setting**:
  1. Wählen Sie in der Dropdownliste einen Stammschlüssel aus.
  2. Geben Sie den Pfad zum Anwendungsordner für den Registrierungs-teilschlüssel ein.
  3. Geben Sie den Name des Schlüsselwertes ein, der gefordert werden soll (optional). Dieser Name wird in der Spalte **Name** des Registrierungs-Editors angezeigt.
  4. Wählen Sie in der Dropdownliste den Typ des Schlüsselwertes aus (Zeichenfolge, Binärwert oder DWORD) (optional). Dieser Typ wird in der Spalte **Type** des Registrierungseditors angezeigt.
  5. Geben Sie den Wert des Schlüsselwertes ein (optional). Diese Informationen werden in der Spalte **Data** des Registrierungseditors angezeigt.

     Wenn der Schlüsselwert für eine Anwendungsversion steht, aktivieren Sie das Kontrollkästchen **Minimum version**, um die angegebene Version oder neuere Versionen der Anwendung zuzulassen. Das IVE verwendet lexikalisches Sortieren, um zu bestimmen, ob der Client die angegebene oder eine neuere Version enthält. Beispiel:

4.0 ist neuer als 3.3	4.1 ist neuer als 3.3.1
4.0a ist neuer als 4.0b	3.3.3 ist neuer als 3.3

     Tipp:

     Verwenden Sie diese Option zum Angeben von Versionsinformationen für eine Antivirenanwendung, um sicherzustellen, dass die Antiviren-software des Clients aktuell ist.
  6. Klicken Sie auf **Save Changes**.

  Hinweis: Wenn Sie lediglich den Schlüssel und den Teilschlüssel angeben, überprüft die Hostprüfung einfach das Vorhandensein des Ordners „Subkey“ in der Registrierung.

7. Wiederholen Sie diesen Vorgang, um eine weitere Regel zur Hostprüfung-Richtlinie hinzuzufügen. Klicken Sie nach dem Hinzufügen der Regeln auf **Save Changes**. Das IVE fügt die Richtlinie der Seite **Configuration** der Hostprüfung hinzu.

☑ Herunterladen des Hostprüfung-Installationsprogramms

Sie können die Anwendung Hostprüfung als ausführbare Windows-Datei herunterladen, die Ihnen folgende Möglichkeiten bietet:

- Verteilen der Datei auf mehrere Clientcomputer mithilfe von Softwareverteilungstools. Mit dieser Option können Sie Hostprüfung auf Clientcomputern installieren, deren Benutzer nicht über die zum Installieren von Hostprüfungerforderlichen Administratorrechte verfügen.
- Bereitstellen der ausführbaren Datei in einem sicheren Repository, damit Benutzer die richtige Version herunterladen und installieren können.

Mit diesen Optionen können Sie steuern, welche Version von Hostprüfung auf Clientcomputern ausgeführt wird.

Wichtig: Wenn Sie die Hostprüfung verteilen, müssen Sie die Option **Auto-upgrade Host Checker** deaktivieren, da das IVE die Hostprüfung sonst auf einen Benutzercomputer herunterlädt, wobei es sich möglicherweise nicht um dieselbe wie die verteilte Version handeln kann.

So laden Sie das Hostprüfung-Installationsprogramm herunter:

1. Wählen Sie in der Webkonsole **System > Configuration > Security > Host Checker** aus.
2. Klicken Sie unter **Policies** auf die Verknüpfung des **Hostprüfung-Installationsprogramms**, um die ausführbare Datei von Hostprüfung vom IVE herunterzuladen.
3. Deaktivieren Sie unter **Options** die Option **Auto-upgrade Host Checker**, um sicherzustellen, dass das IVE die Hostprüfung nicht auf Clients herunterlädt, und klicken Sie dann auf **Save Changes** (optional).

Registerkarte „Security > Cache Cleaner“

Geben Sie auf der Registerkarte **System > Configuration > Security > Cache Cleaner** (Cachebereinigung) an, ob die Cachebereinigung ausgeführt und das IVE über ihren Status informiert wird. Geben Sie außerdem zu löschende Cachedaten des Browsers und Verzeichnisdaten an. Weitere Informationen über diese Funktion finden Sie unter „Cachebereinigung – Übersicht“ auf Seite 63.

☑ Angeben globaler Einstellungen für die Cachebereinigung

So geben Sie globale Einstellungen für die Cachebereinigung an:

1. Wählen Sie in der Webkonsole **System > Configuration > Security > Cachebereinigung** aus.
2. Führen Sie im oberen Bereich der Seite Folgendes aus:
    1. Geben Sie die **Cleaner Frequency** an, um zu bestimmen, wie oft die Cachebereinigung ausgeführt wird. Bei jeder Ausführung der Cachebereinigung löscht sie den Cache des Browsers und die Dateien und Ordner, die Sie unten in den Bereichen **Browser Cache** und **Files and Folders** angeben.
    2. Geben Sie die **Status Update Frequency** an, um zu bestimmen, wie oft das IVE erwartet, dass die Cachebereinigung sich selbst aktualisiert.
    3. Aktivieren Sie das Kontrollkästchen **Uninstall Cache Cleaner at logout**, wenn das IVE die Cachebereinigung beim Beenden einer Benutzersitzung vom Clientcomputer deinstallieren soll (optional).
3. Geben Sie unter **Browser Cache** einen oder mehrere Hostnamen oder Domänen ein (Platzhalter sind zulässig). Beim Beenden einer Benutzersitzung entfernt die Cachebereinigung den gesamten Inhalt des Browsercaches, der von diesen Servern stammt. Die Cachebereinigung entfernt diesen Inhalt auch, wenn sie im angegebenen Bereinigungsintervall ausgeführt wird.

    Hinweis: Das IVE löst Hostnamen nicht auf. Geben sie deshalb alle möglichen Angaben eines Servers wie dessen Hostnamen, FQDN und IP-Adresse an.

4. Führen Sie unter **Files and Folders** Folgendes aus:
   1. Geben Sie eine der folgenden Informationen an:
      - den Namen der Datei, die von der Cachebereinigung entfernt werden soll, oder
      - den vollständigen Verzeichnispfad zu einem Ordner, dessen Inhalt von der Cachebereinigung entfernt werden soll. Wenn Sie ein Verzeichnis angeben, wählen Sie **Clear Subfolders** aus, um auch den Inhalt aller Unterverzeichnisse in diesem Verzeichnis zu löschen.
   2. Aktivieren Sie das Kontrollkästchen **Clear folders only at the end of session**, wenn die Cachebereinigung den Verzeichnisinhalt nur nach dem Beenden der Benutzersitzung löschen soll. Andernfalls löscht die Cachebereinigung auch Dateien und Ordner im angegebenen Bereinigungsintervall.
5. Klicken Sie zum globalen Speichern der Einstellungen auf **Save Changes**.

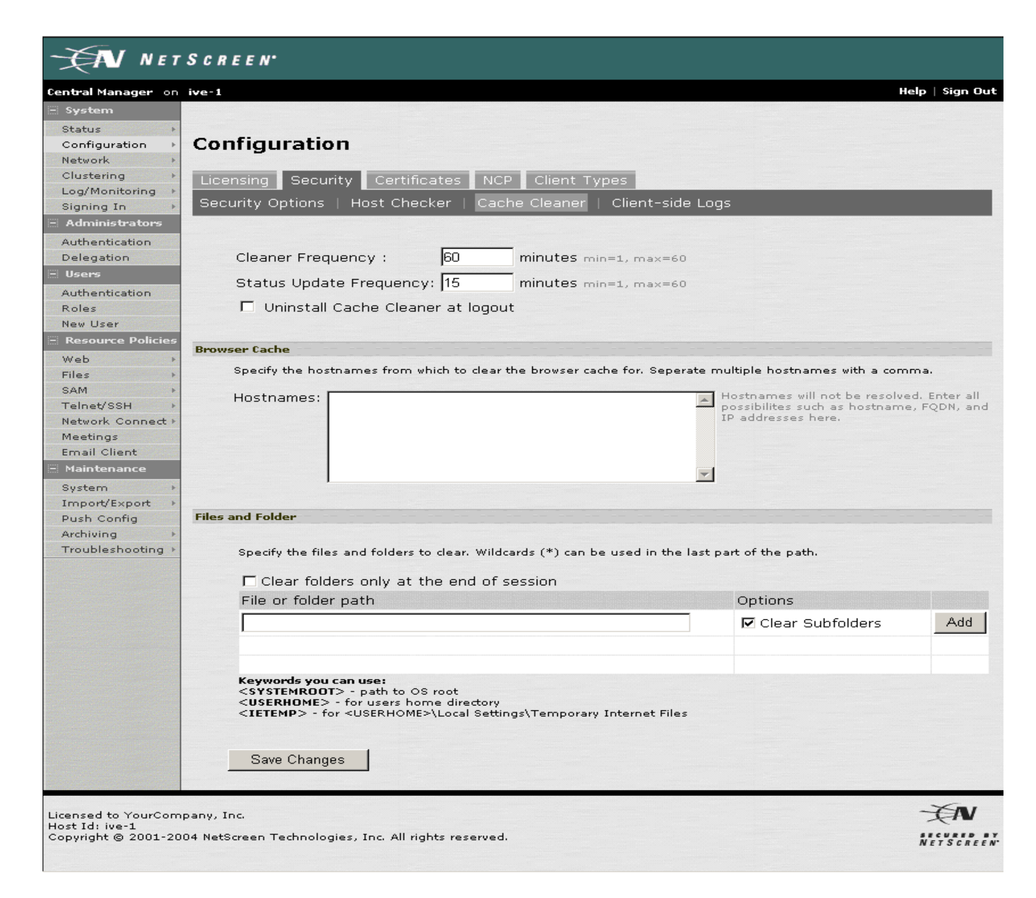


Abbildung 22: **System > Configuration > Security > Cache Cleaner**

Registerkarte „Security > Client-side Logs“

Auf der Registerkarte **System > Configuration > Security > Client-side Logs** können Sie clientseitige Protokollierung für die Funktionen zur Hostprüfung, Cachebereinigung und für Secure Meeting aktivieren. Wenn Sie diese Option für eine Funktion aktivieren, schreibt das IVE ein verschlüsseltes clientseitiges Protokoll für jeden Client, der diese Funktion verwendet. Bei jedem Aufruf dieser Funktion in nachfolgenden Benutzersitzungen fügt das IVE Informationen zur Protokolldatei hinzu. Diese Funktion ist bei der Zusammenarbeit mit dem Support-Team nützlich, um mit der entsprechenden Funktion zusammenhängende Probleme zu debuggen.

Wichtig: Da diese Einstellungen global sind, schreibt das IVE eine Protokolldatei für alle Clients, die die Funktion verwenden, für die Sie die clientseitige Protokollierung aktivieren. Außerdem entfernt das IVE keine clientseitigen Protokolle. Benutzer müssen Protokolldateien manuell von ihren Clients löschen. Diese Dateien sind durch eine `.log`-Erweiterung gekennzeichnet und sind in Verzeichnissen gespeichert, die der Funktion in `C:\Programme\Neoteris` entsprechen.

☑ Festlegen von Einstellungen für clientseitige Protokollierung

So legen Sie Einstellungen für clientseitige Protokollierung fest:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Security > Client-side Logs** aus.
2. Wählen Sie die gewünschten Funktionen aus, für die das IVE client-seitige Protokolle schreibt. Folgende Optionen stehen zur Verfügung:
   - Hostprüfung – Das IVE schreibt `dsHostChecker.log` in `C:\Programme\Neoteris\Host Checker`.
   - Cachebereinigung – Das IVE schreibt `dsCacheCleaner.log` in `C:\Programme\Neoteris\Cache Cleaner`.
   - Meetings – Das IVE schreibt `dsCboxUI.log` oder `NeoterisSetup.log`. Der Speicherort dieser Dateien hängt von der Systemkonfiguration des Benutzers ab. Führen Sie für die einzelnen Benutzer Folgendes aus:
     - Windows-Benutzer mit Administrator- oder Hauptbenutzerberechtigungen: `C:\Programme\Neoteris\Secure Meeting <Versionsnummer>\dsCboxUI.log oder C:\Windows -oder- WINNT\Übertragene Programmdateien\NeoterisSetup.log`

- Windows-Benutzer mit Standardberechtigungen: `C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\Neoteris\Secure Meeting <Versionsnummer>\dsCboxUI.log` oder `C:\ Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\Neoteris\setup\NeoterisSetup.log` -und- `NeoterisSetupApp.log`
- Macintosh- oder Linux-Benutzer: `\tmp\dsCboxUI.log`.

3. Klicken Sie zum globalen Speichern der Einstellungen auf **Save Changes**.

Hinweis: Für neue IVE 4.x-Systeme sind alle drei Optionen standardmäßig *deaktiviert*. Wenn Sie Ihr IVE von einer 3.x-Konfiguration aktualisieren, sind alle drei Protokolloptionen standardmäßig *aktiviert*.

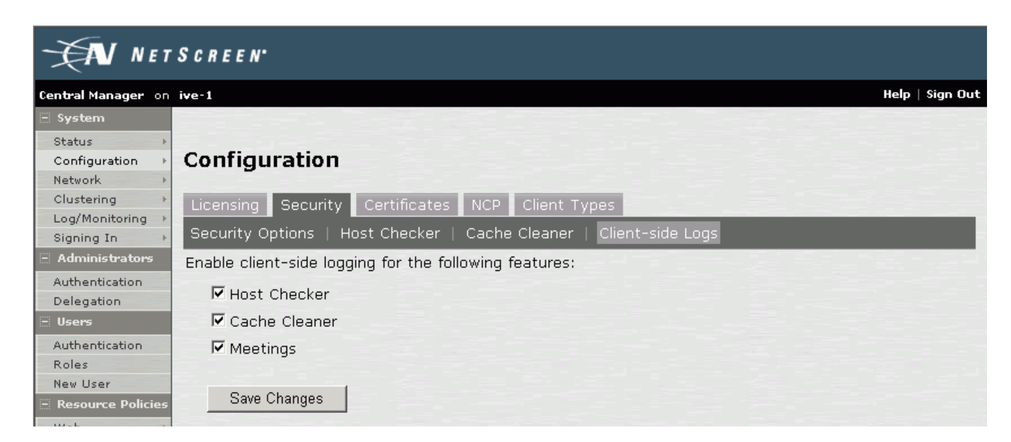


Abbildung 23: **System > Configuration > Security > Client-side Logs**

Registerkarte „Certificates > Server Certificates“

Das IVE unterstützt X.509-Server-Zertifikate, die mit DER oder PEM (u. a. die Dateierweiterungen .cer, .crt, .der und .pem) bzw. PKCS #12 (Dateierweiterungen u. a. .pfx und .p12) codiert sind.

Auf der Registerkarte **System > Configuration > Certificates > Server Certificate** können Sie Folgendes ausführen:

☑ Importieren eines vorhandenen Zertifikats und eines privaten Schlüssels

Sie können Webserverzertifikate von Servern wie Apache, IIS, Sun ONE (früher iPlanet) oder Netscape erstellen und das Zertifikat dann in das IVE importieren. Zum Exportieren eines digitalen Serverzertifikats und eines Schlüssels befolgen Sie die zu dem Webserver vorhandenen Anweisungen zum Exportieren von Zertifikaten. Importieren Sie anschließend diese Dateien über die Registerkarte **Server Certificates**.

Wichtig:

- Beachten Sie beim Exportieren eines Zertifikats von einem anderen Webserver, dass es verschlüsselt sein muss und dass Sie das Kennwort mit dem Zertifikat exportieren müssen.
- Sie können den privaten Schlüssel eines Webserverzertifikats nicht in ein Access Series FIPS-Gerät importieren, da dieser Schlüssel in einer Umgebung erzeugt wird, die nicht mit FIPS kompatibel ist. Sie können aber einen Zertifikatsschlüssel zusammen mit der Security World von einem anderen IVE importieren. Weitere Informationen finden Sie unter „Importieren einer Systemkonfigurationsdatei“ auf Seite 531.

So importieren Sie ein vorhandenes digitales Serverzertifikat und einen privaten Schlüssel:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates** > **Server Certificates** aus.
2. Klicken Sie auf **Import Certificate & Key**.
3. Wählen Sie das entsprechende Formular für den Import des Zertifikats aus:
   - Falls das Zertifikat und der Schlüssel in einer Datei enthalten sind, verwenden Sie das Formular **Certificate file includes private key**.
   - Handelt es sich bei dem Zertifikat und dem Schlüssel um separate Dateien, verwenden Sie das Formular **Certificate and private key are separate files**.
4. Wechseln Sie im entsprechenden Formular zu der Datei mit dem Zertifikat und dem Schlüssel. Wenn die Datei verschlüsselt ist, geben Sie den Kennwortschlüssel ein.
5. Klicken Sie auf **Import**.

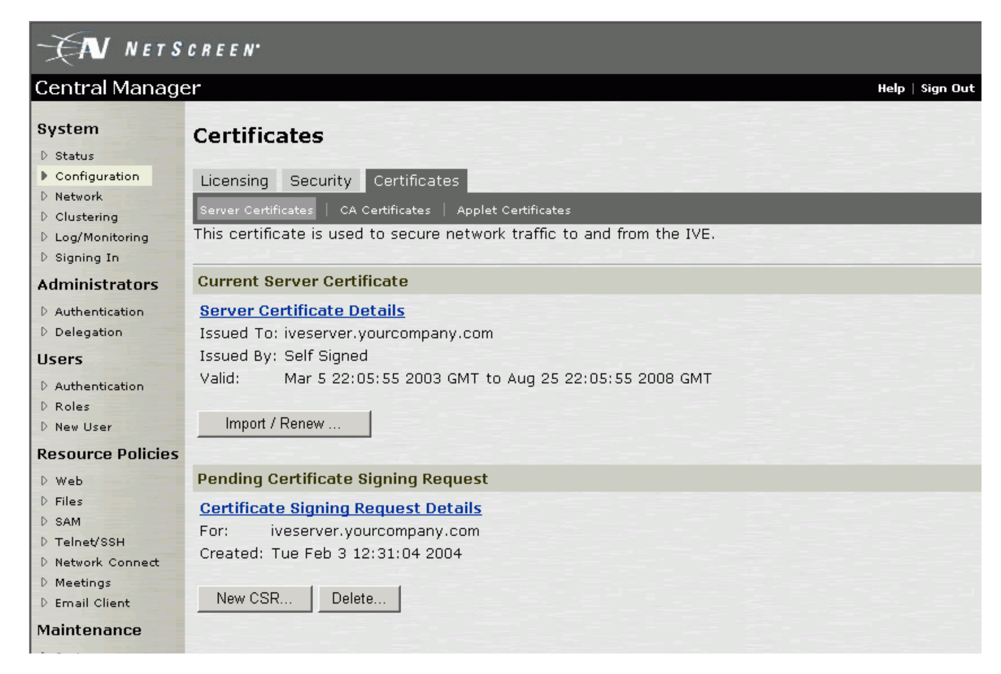


Abbildung 24: **System > Configuration > Certificates > Server Certificates**

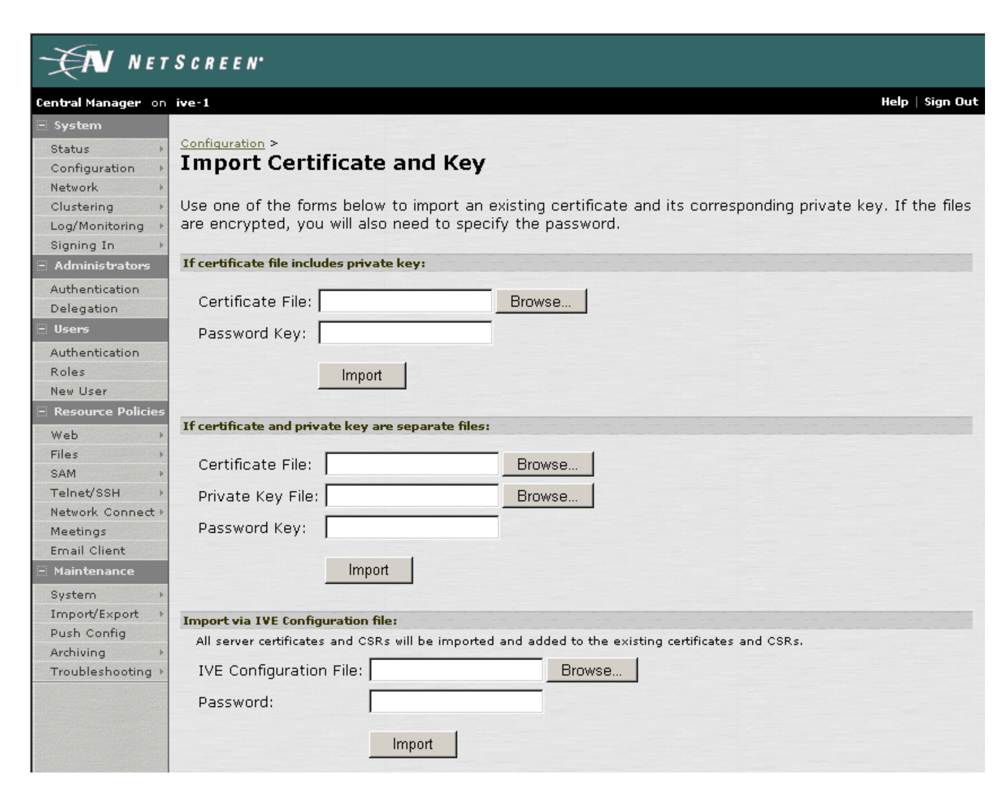


Abbildung 25: **System > Configuration > Certificates > Server Certificates > Import Certificate & Key**

☑ Importieren eines erneuerten Zertifikats, das den vorhandenen privaten Schlüssel verwendet:

Sie können ein Serverzertifikat auf zwei Arten erneuern:

- **Bei einer Zertifizierungsstelle eine neue Zertifikatssignaturanforderung einreichen**

  Dieser Vorgang zur Erneuerung eines Zertifikats ist sicherer, da die Zertifizierungsstelle ein neues Zertifikat und einen neuen privaten Schlüssel generiert und dabei die Gültigkeit des älteren privaten Schlüssels aufhebt. Zur Verwendung dieser Erneuerungsmethode müssen Sie zuerst über die Webkonsole eine Zertifikatssignaturanforderung erstellen. Weitere Informationen finden Sie unter „Erstellen einer Zertifikatssignaturanforderung für ein neues Zertifikat“ auf Seite 187.

  Wichtig: Sie können den privaten Schlüssel eines Webserverzertifikats nicht auf ein Access Series FIPS-Gerät importieren, da dieser Schlüssel in einer Umgebung erzeugt wird, die nicht mit FIPS kompatibel ist.

- **Basierend auf der vorher bei der Zertifizierungsstelle eingereichten Zertifikatssignaturanforderung eine Erneuerung anfordern**

  Dieser Vorgang zur Erneuerung eines Zertifikats ist weniger sicher, da die Zertifizierungsstelle ein Zertifikat generiert, das den vorhandenen privaten Schlüssel verwendet.

  Wichtig: Wenn Sie ein erneuertes Zertifikat anfordern, müssen Sie Ihre ursprüngliche Zertifikatssignaturanforderung erneut senden, um sicherzustellen, dass die Zertifizierungsstelle über einen Datensatz für die Zertifikatssignaturanforderung verfügt, die Sie für Ihr aktuelles Zertifikat gesendet haben.

So importieren Sie ein erneuertes Serverzertifikat, das den vorhandenen privaten Schlüssel verwendet

1. Befolgen Sie die Anweisungen der Zertifizierungsstelle zur Erneuerung eines Zertifikats, das Sie zuvor dort erworben haben.

   Wichtig: Vergewissern Sie sich, dass Sie dieselben Informationen angeben, die in der ursprünglichen Zertifikatssignaturanforderung verwendet wurden. Anhand dieser Informationen erstellt die Zertifizierungsstelle ein neues Zertifikat, das dem vorhandenen Schlüssel entspricht.

   ---

2. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates** > **Server Certificates** aus. (**Abbildung 24** auf Seite 181)
3. Klicken Sie auf die Verknüpfung, die dem zu erneuernden Zertifikat entspricht. (**Abbildung 25** auf Seite 182)
4. Klicken Sie auf **Renew Certificate**.
5. Navigieren Sie im Formular **Renew the Certificate** zu der erneuerten Zertifikatsdatei, geben Sie das Kennwort für den Zertifizierungsschlüssel ein, und klicken Sie auf **Import**.

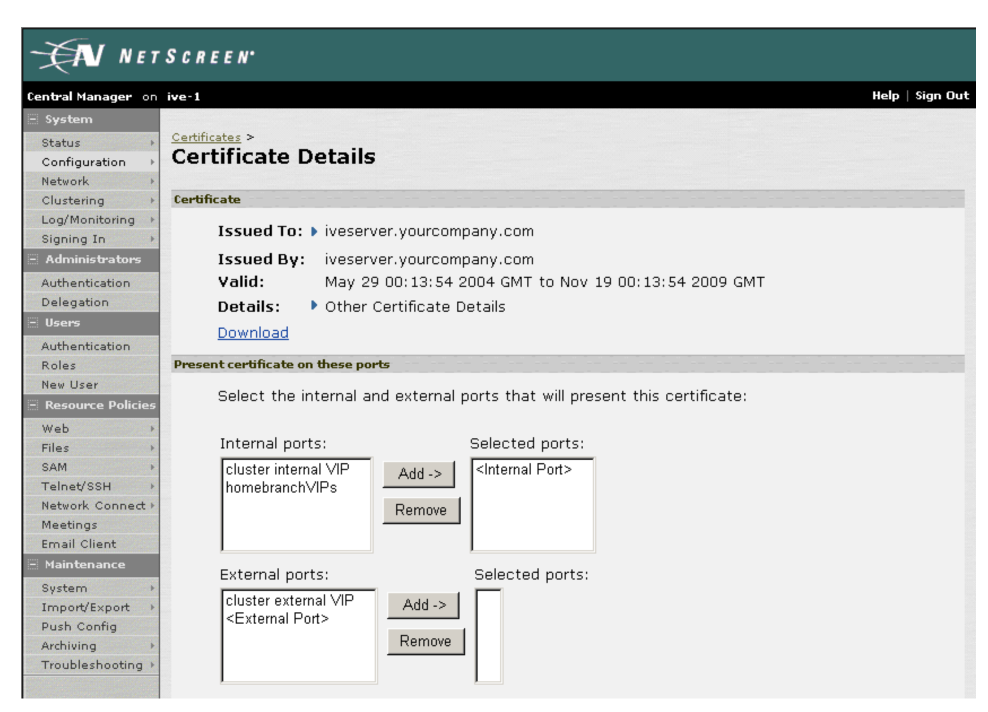


Abbildung 26: **System > Configuration > Certificates > Server Certificates > Certificate Details**

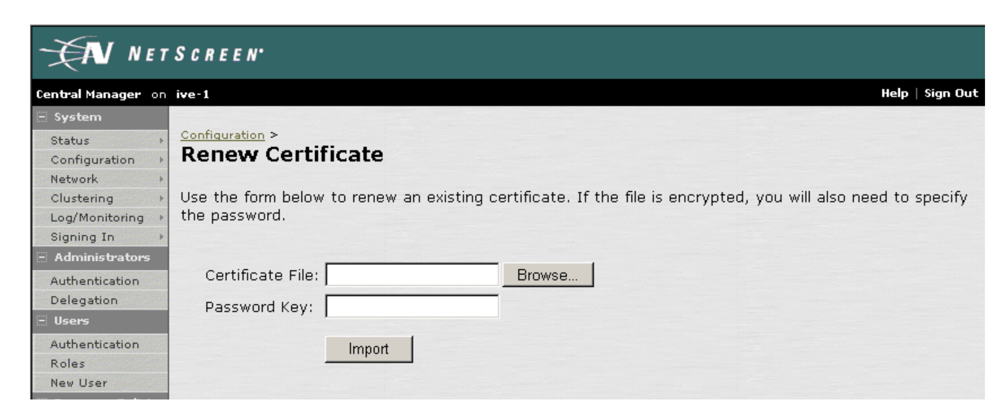


Abbildung 27: **System > Configuration > Certificates > Server Certificates > Renew Certificate**

☑ Herunterladen eines Serverzertifikats und eines privaten Schlüssels vom IVE

Wenn Sie eine SAML-Ressourcenrichtlinie erstellen, müssen Sie eine Vertrauensstellung zwischen dem IVE und Ihrem Zugriffsverwaltungs-system erstellen. (Vertrauensstellungen gewährleisten, dass SAML-fähige Systeme nur Informationen von und an vertrauenswürdige Quellen weitergeben.) Wenn Sie eine SAML SSO-Ressourcenrichtlinie mit einem POST-Profil erstellen möchten, müssen Sie beim Erstellen einer Vertrauens-stellung das Serverzertifikat des IVE auf dem Zugriffs-verwaltungssystem installieren. Über die Seite **Server Certificates** können Sie auf einfache Weise das Zertifikat des IVE herunterladen, um es auf Ihrem Zugriffs-verwaltungssystem zu installieren.

So laden Sie ein Serverzertifikat vom IVE herunter:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates** > **Server Certificates** aus. (**Abbildung 24** auf Seite 181)
2. Klicken Sie auf die Verknüpfung, die dem zu speichernden Zertifikat entspricht. (**Abbildung 25** auf Seite 182)
3. Klicken Sie auf **Download**.
4. Navigieren Sie zu dem Speicherort, an dem Sie das Zertifikat speichern möchten, und klicken Sie auf **Save**.

☑ Zuordnen eines Zertifikats zu einem virtuellen Port

Wenn Sie einem einzelnen IVE mehrere Hostnamen zuordnen möchten, müssen Sie angeben, welche Zertifikate das IVE verwenden soll, um Benutzer zu überprüfen, die sich bei den verschiedenen Hostnamen anmelden. Folgende Optionen stehen zur Verfügung:

- **Zuordnen aller Hostnamen zu einem einzelnen Platzhalterzertifikat**

  Bei dieser Methode verwenden Sie ein einzelnes Platzhalterzertifikat, um alle Benutzer zu überprüfen, unabhängig davon, welchen Hostnamen sie verwenden, um sich beim IVE anzumelden. Ein ***Platzhalterzertifikat*** schließt im Domänennamen ein variables Element ein, wodurch es Benutzern, die sich von mehreren Hosts anmelden, ermöglicht wird, sich der „gleichen" Domäne zuzuordnen. Wenn Sie z. B. ein Platzhalter-zertifkat für `*.eigenefirma.de` erstellen, verwendet das IVE zum Authentifizieren von Benutzern, die sich bei `mitarbeiter.eigenefirma.de` anmelden, das gleiche Zertifikat wie zum Authentifizieren von Benutzern, die sich bei `partner.eigenefirma.de` anmelden.

- **Zuordnen jedes Hostnamens zu seinem eigenen Zertifikat**

  Bei dieser Methode ordnen Sie verschiedene Hostnamen verschiedenen Zertifikaten zu. Da allerdings dem IVE der Hostname, mit dem sich der Endbenutzer bei diesem anmeldet, nicht bekannt ist, müssen Sie einen virtuellen Port für jeden Hostnamen erstellen und dann Ihre Zertifikate den virtuellen Ports zuordnen. Ein ***virtueller Port*** aktiviert einen IP-Alias für einen physischen Port. Sie können beispielsweise zwei virtuelle Ports für eine einzige Appliance erstellen, wobei Sie dem ersten virtuellen Port die IP-Adresse 10.10.10.1 (`vertrieb.eigenefirma.com`) und dem zweiten virtuellen Port die IP-Adresse 10.10.10.2 (`partner.eigenefirma.com`) zuordnen. Anschließend können Sie jedem dieser virtuellen Ports ein eigenes Zertifikat zuordnen, um sicherzustellen, dass das IVE verschiedene Benutzer über unterschiedliche Zertifikate authentifiziert.

So ordnen Sie verschiedene Zertifikate verschiedenen virtuellen Ports zu:

1. Navigieren Sie in der Webkonsole zur Registerkarte **System > Network > Internal Port** (Seite 212) oder zur Registerkarte **External Port** (Seite 212). Erstellen Sie dann über die Seite **Virtual Ports** Ihre virtuellen Ports.
2. Importieren Sie die Serverzertifikate, die Sie zum Überprüfen von Benutzerzertifikaten verwenden möchten. Sie können Zertifikate von der Seite **System > Configuration > Certificates > Server Certificates** der Webkonsole (Seite 179) oder von der Seite **Maintenance > Import/Export > System Configuration** der Webkonsole importieren (Seite 530).
3. Klicken Sie auf der Seite **System > Configuration > Certificates > Server Certificates** auf die Verknüpfung, die einem Zertifikat entspricht, das Sie zum Überprüfen von Benutzerzertifikaten verwenden möchten. (**Abbildung 25** auf Seite 182)
4. Geben Sie unter **Present certificate on these ports** den Port oder die Ports an, den bzw. die das IVE dem Zertifikat zuordnen soll. Sie können interne oder externe Ports bzw. primäre oder virtuelle Ports wählen, aber keinen Port, der bereits einem anderen Zertifikat zugeordnet ist. (**Abbildung 26** auf Seite 184)
5. Klicken Sie auf **Save Changes**.
6. Wiederholen Sie die Schritte 3-6 für jedes der Zertifikate, das Sie zum Authentifizieren von Benutzern verwenden möchten.

☑ Erstellen einer Zertifikatssignaturanforderung für ein neues Zertifikat

Falls Ihr Unternehmen über kein digitales Zertifikat für die Webserver verfügt oder Sie ein Access Series FIPS-Gerät betreiben, können Sie über die Webkonsole eine Zertifikatssignaturanforderung erstellen und diese dann zur Verarbeitung an eine Zertifizierungsstelle senden. Wenn Sie über die Webkonsole eine Zertifikatssignaturanforderung erstellen, wird lokal ein privater Schlüssel erstellt, der der Zertifikatssignaturanforderung entspricht. Falls Sie die Zertifikatssignaturanforderung löschen, wird diese Datei ebenfalls gelöscht. Es ist dann nicht mehr möglich, ein über die Zertifikatssignaturanforderung erstelltes signiertes Zertifikat zu installieren.

Wichtig: Senden Sie nur jeweils eine Zertifikatssignaturanforderung an eine Zertifizierungsstelle. Andernfalls fallen u. U. doppelte Gebühren an. Sie können Details zu zuvor gesendeten, ausstehenden Anforderungen anzeigen, indem Sie auf die Verknüpfung **Certificate Signing Request Details** auf der Registerkarte **Server Certificates** klicken.

So erstellen Sie eine Zertifikatssignaturanforderung:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Server Certificates** aus. (**Abbildung 24** auf Seite 181)
2. Klicken Sie unter **Certificate Signing Requests** auf **New CSR**.
3. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Create CSR**.
4. Klicken Sie unter **Certificate Signing Requests** auf die Verknüpfung **Pending CSR** für die soeben erstellte Zertifikatssignaturanforderung.
5. Folgen Sie den Anweisungen auf dem Bildschirm. Darin wird neben dem Sendeverfahren erläutert, welche Informationen an die Zertifizierungsstelle gesendet werden müssen.
6. Wenn Sie von der Zertifizierungsstelle ein signiertes Zertifikat erhalten, importieren Sie anhand der folgenden Anweisungen die Zertifikatdatei.

Hinweis: Wenn Sie eine Zertifikatssignaturanforderung bei einer Zertifizierungsstelle einreichen, werden Sie u. U. dazu aufgefordert, entweder den Typ des Webservers anzugeben, auf dem das Zertifikat erstellt wurde, oder den Typ des Webservers, für den das Zertifikat bestimmt ist. Wählen Sie **apache** aus (falls mehrere Optionen mit „apache“ verfügbar sind, wählen Sie eine beliebige aus). Wählen Sie außerdem, falls Sie zur Auswahl des Formats des herunterzuladenden Zertifikats aufgefordert werden, das Standardformat aus.

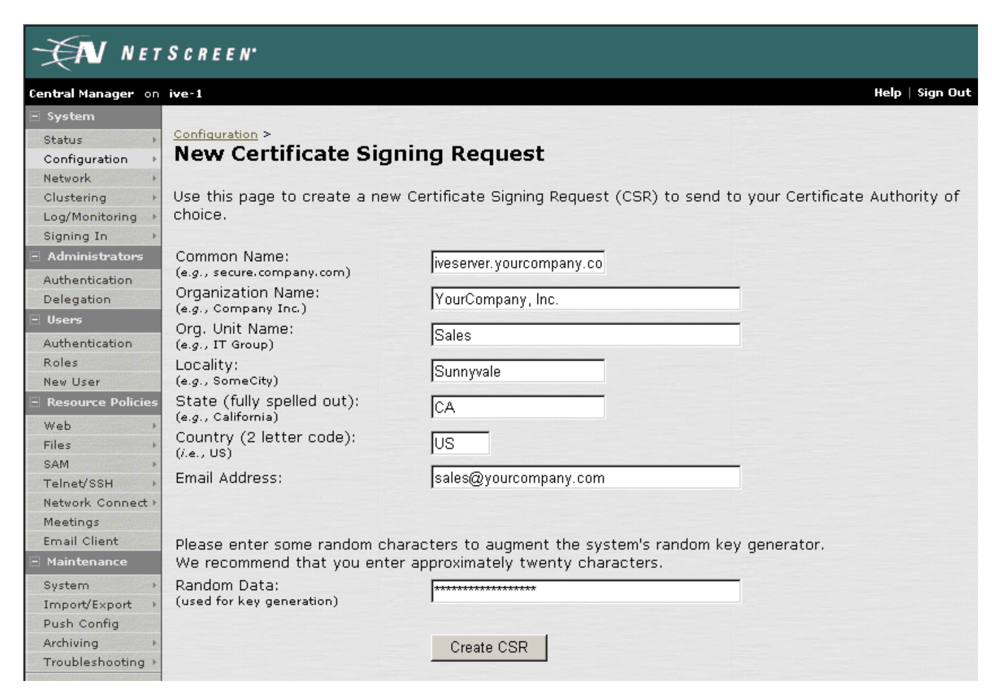


Abbildung 28: **System > Configuration > Certificates > Server Certificates > New Certificate Signing Request**

☑ Importieren eines signierten Zertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde

Wenn Sie über die Webkonsole eine Zertifikatssignaturanforderung erstellen, zeigt das IVE auf der Registerkarte **Server Certificates** eine Verknüpfung **Pending CSR** für die Zertifikatssignaturanforderung an, bis Sie das von der Zertifizierungsstelle verteilte signierte Serverzertifikat importieren.

So importieren Sie ein signiertes Serverzertifikat, das anhand einer Zertifikatssignaturanforderung erstellt wurde:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > Server Certificates** aus. (**Abbildung 24** auf Seite 181)
2. Klicken Sie unter **Certificate Signing Requests** auf die Verknüpfung **Pending CSR**, die dem signierten Zertifikat entspricht.
3. Navigieren Sie unter **Import signed certificate** zu der Zertifikatdatei, die Sie von der Zertifizierungsstelle erhalten haben, und klicken Sie dann auf **Import**.

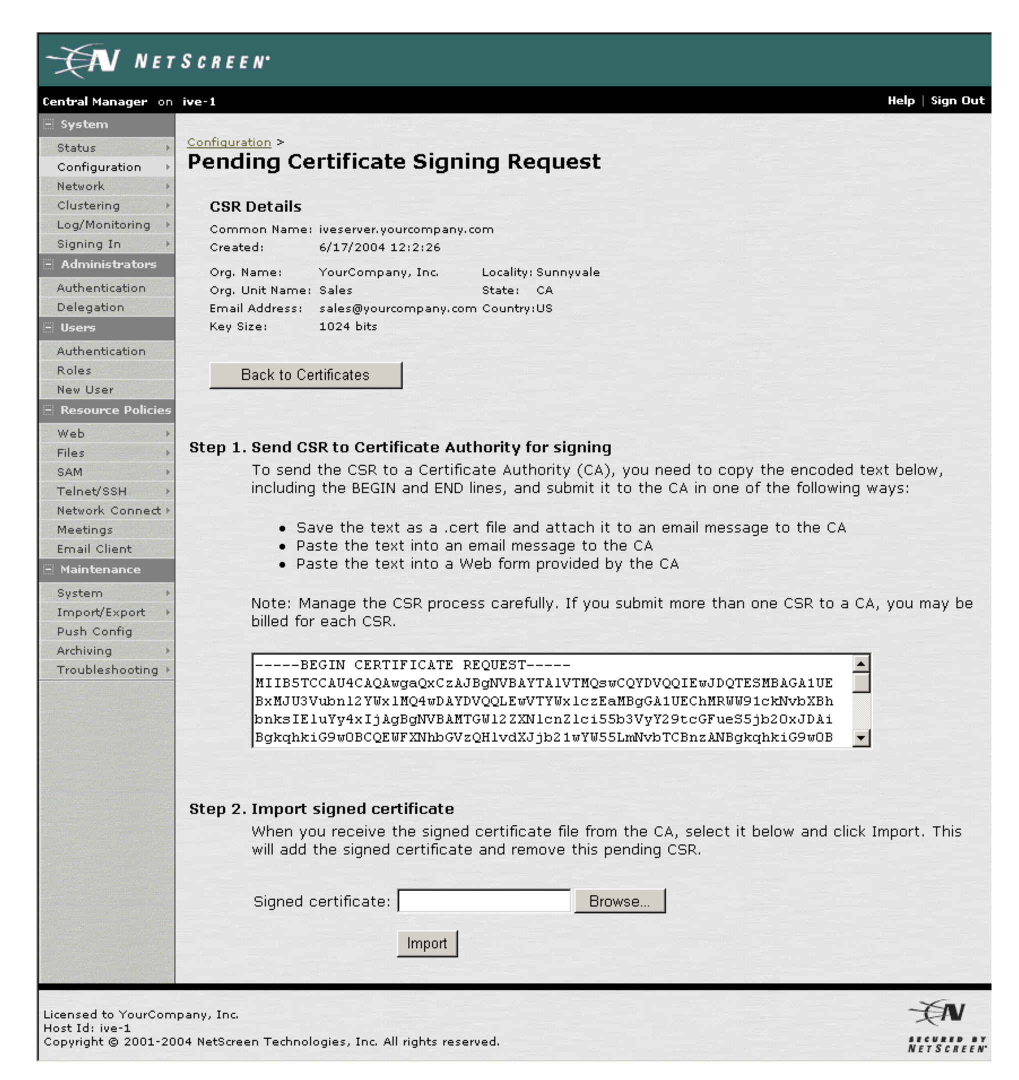


Abbildung 29: System > Configuration > Certificates > Server Certificates > Pending Certificate Signing Request

Registerkarte „Certificates > CA Certificates“

Auf der Registerkarte **System > Configuration > Certificates > CA Certificate** können Sie Zertifikate der Zertifizierungsstelle importieren und Optionen für diese konfigurieren. Das IVE unterstützt X.509-Zertifikate, die in DER- und PEM-Formaten codiert sind.

Dieser Abschnitt umfasst folgende Aufgaben:

☑ Hochladen von Zertifikaten der Zertifizierungsstelle auf das IVE

Wenn Sie bestimmen, dass Benutzer zum Anmelden am IVE ein clientseitiges Zertifikat bereitstellen müssen, müssen Sie das entsprechende Zertifikat der Zertifizierungsstelle auf das IVE hochladen. Das IVE verwendet das hochgeladene Zertifikat zum Überprüfen, ob das vom Browser bereitgestellte Zertifikat gültig ist.

Wichtig:

- Bei Verwendung clientseitiger Zertifikate ist dringend zu empfehlen, die Benutzer anzuweisen, ihre Webbrowser nach dem Abmelden vom IVE zu schließen. Andernfalls können andere Benutzer über deren geöffnete Browsersitzungen auf durch Zertifikate geschützte Ressourcen auf dem IVE ohne erneute Authentifizierung zugreifen. (Nach dem Laden eines clientseitigen Zertifikats werden die Anmeldinformationen und der private Schlüssel des Zertifikats von Internet Explorer und Netscape zwischengespeichert. Diese Informationen bleiben in den Browsern zwischengespeichert, bis der Browser vom Benutzer geschlossen wird (in manchen Fällen, bis die Arbeitsstation neu gestartet wird). Ausführliche Informationen finden Sie unter: `http://support.microsoft.com/?kbid=290345`. Sie können Benutzer daran erinnern, ihren Browser zu schließen, indem Sie die Meldung für die Abmeldung auf der Registerkarte **System > Signing In > Sign-in Pages** ändern (Seite 274).
- Durch das Hochladen eines Zertifizierungsstelleszertifikats auf das IVE wird die clientseitige SSL-Authentifizerung nicht aktiviert. Sie müssen entweder einen Zertifikatserver verwenden (Seite 299) oder auf der Seite **Administrators/Users > Authentication > [Bereich] > Authentication Policy > Certificate** der WebkonsoleZertifikatein-schränkungen aktivieren, um die clientseitige SSL-Authentifizierung zu aktivieren.

- Beim Hochladen einer Zertifikatkette auf das IVE müssen Sie entweder beginnend mit dem Stammzertifikat die Zertifikate einzeln in absteigender Reihenfolge installieren (DER- oder PEM-Dateien) oder eine einzelne Datei auf das IVE hochladen, die die gesamte Zertifikatkette enthält (nur PEM-Dateien). Durch Verwenden einer dieser Methoden stellen Sie sicher, dass das IVE die Zertifikate in der richtigen Reihenfolge miteinander verknüpft.

So laden Sie Zertifizierungsstellenzertifikate auf das IVE hoch:

1. Installieren Sie ein clientseitiges Zertifikat über den Browser des Benutzers. Hilfe dazu können Sie den Anweisungen zu dem Browser entnehmen.
2. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Certificates > CA Certificates** aus.
3. Klicken Sie auf **Import CA Certificate**.
4. Navigieren Sie zum Zertifizierungsstellenzertifikat, das Sie auf das IVE hochladen möchten, und klicken Sie auf **Import Certificate**.
5. Bestimmen Sie, welche Bereiche das Zertifikat zum Authentifizieren von Benutzern verwenden sollen, und aktivieren Sie dann mit den Einstellungen auf der Registerkarte **Users > Authentication > [Bereich] > Authentication Policy > Certificate** das Zertifikat für diese Bereiche.
6. Verwenden Sie die Anweisungen in Anhang B, um X.509-DN-Attribute (Distinguished Name) anzugeben, die Benutzer zur Authentifizierung, zum Rollen- bzw. Ressourcenrichtlinienzugriff oder zum Aktivieren der Zertifikatauthentifizierung für Administratorbereiche zusätzlich zu Benutzerbereichen bereitstellen müssen (optional).

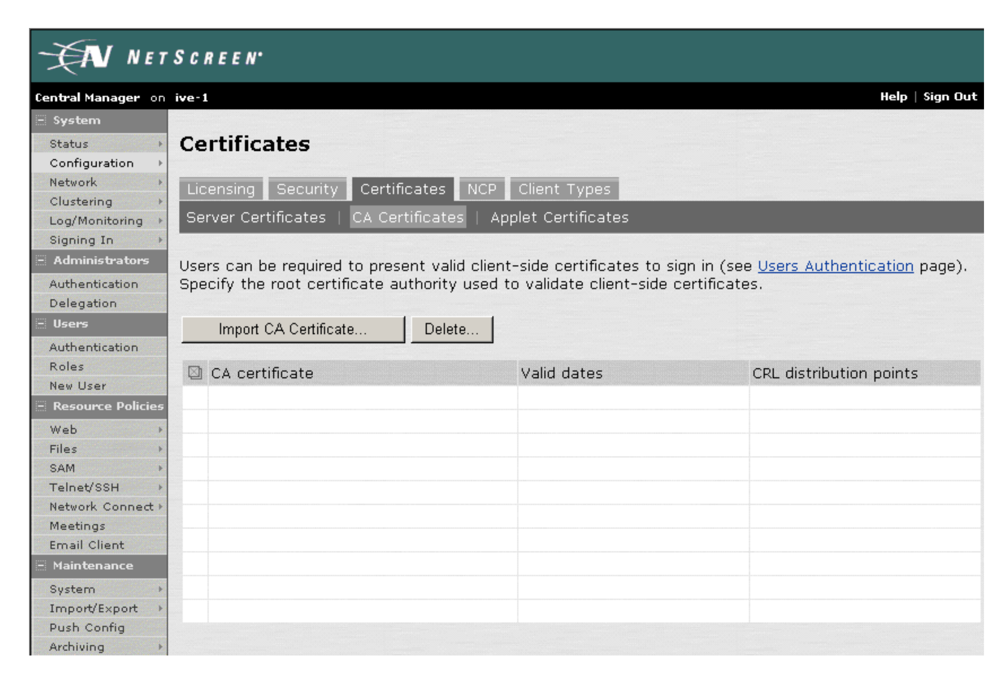


Abbildung 30: **System > Configuration > Certificates > CA Certificates**

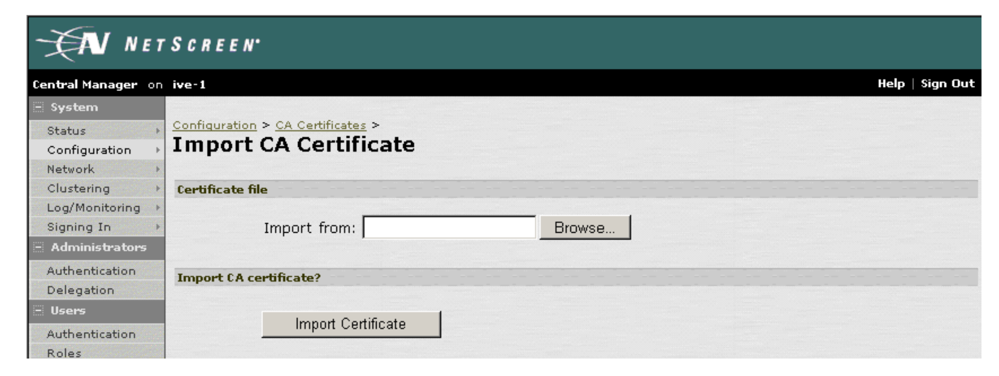


Abbildung 31: **System > Configuration > Certificates > CA Certificates > Import Certificate**

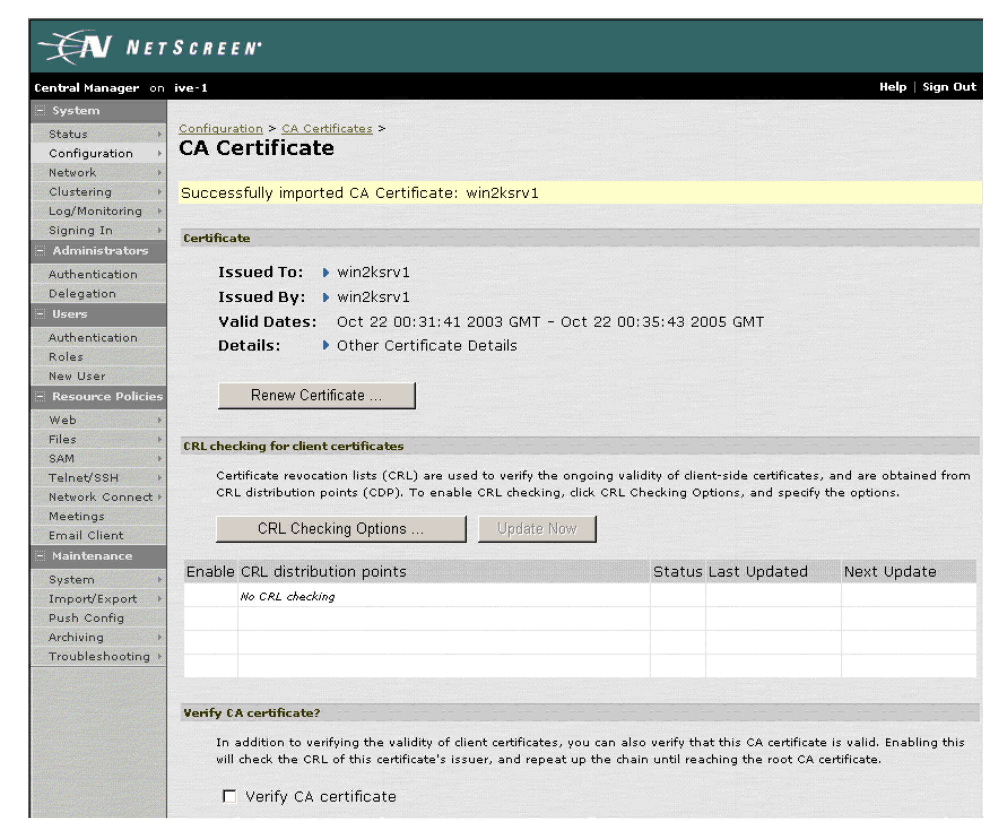


Abbildung 32: **System > Configuration > Certificates > CA Certificates > Import Certificate > CA Certificate**

☑ Erneuern eines Zertifizierungsstellenzertifikats

Zum Erneuern eines Zertifizierungsstellenzertifikats muss Ihre Zertifizierungsstelle ein neues Zertifikat ausstellen, das den gleichen privaten Schlüssel verwenden wie Ihr vorhandenes Zertifikat, und dann das neue Zertifikat auf das IVE hochladen.

So importieren Sie ein erneuertes Zertifizierungsstellenzertifikat in das IVE:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > CA Certificate** aus. (**Abbildung 30** auf Seite 192)
2. Klicken Sie auf die Verknüpfung, die dem zu erneuernden Zertifikat entspricht. (**Abbildung 32** auf Seite 193)

3. Klicken Sie auf **Renew Certificate**.
4. Navigieren Sie zum Zertifizierungsstellenzertifikat, das Sie auf das IVE hochladen möchten, und klicken Sie auf **Import Certificate**.

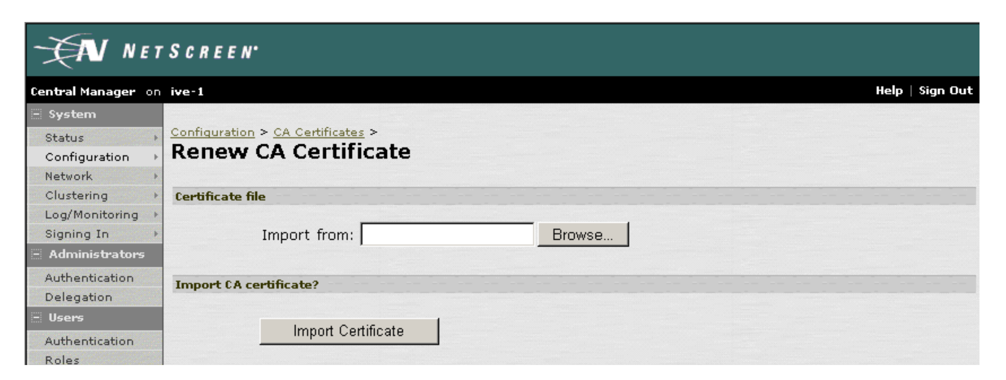


Abbildung 33: **System > Configuration > Certificates > CA Certificates > Renew CA Certificate**

☑ Aktivieren der CRL-Prüfung

Sie können Zertifikatsperrlisten (Certificate Revocation List, CRL) aktivieren und regelmäßig von Sperrlisten-Verteilungspunkten (CRL Distribution Points, CDPs) herunterladen, um die dauerhafte Gültigkeit der clientseitigen Zertifikate sicherzustellen.

So aktivieren Sie die CRL-Überprüfung:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > CA Certificate** aus. (**Abbildung 30** auf Seite 192)
2. Klicken Sie auf die Verknüpfung, die dem Zertifikat entspricht, für das Sie die CRL-Überprüfung aktivieren möchten. (**Abbildung 32** auf Seite 193)
3. Klicken Sie auf **CRL Checking Options**.

4. Geben Sie unter **CRL Distribution Points** an, wo das IVE Zugriffsinformationen für den Sperrlisen-Verteilungspunkt finden kann. Folgende Optionen stehen zur Verfügung:
   - **No CDP (no CRL Checking)**

     Wenn Sie diese Option auswählen, überprüft das IVE von der Zertifizierungsstelle ausgestellte CRLs nicht. Deshalb müssen Sie keine Parameter für den Zugriff auf den Sperrlisten-Verteilungspunkt eingeben, der die CRL ausgestellt hat.
   - **CDP(s) specified in the CA Certificate**

     Wenn Sie diese Option auswählen, überprüft das IVE das CRL-Verteilungspunktattribut im Zertifikat und zeigt die URIs der Sperrlisten-Verteilungspunkte an, die es auf der Seite **CRL Checking Options** findet. Wenn das Zertifizierungsstellenzertifikat nicht alle für den Zugriff auf den Sperrlisten-Verteilungspunkt benötigten Informationen enthält, geben Sie die zusätzlich erforderlichen Informationen an:
     - **CDP Server:** (nur LDAP) Geben Sie den Ort des CDP-Servers ein. Geben Sie bei Verwendung des LDAP-Protokolls die IP-Adresse oder den Hostnamen ein (z. B. `ldap.domain.com`).
     - **CRL Attribute:** (nur LDAP) Geben Sie das LDAP-Atttibut für das Objekt ein, das den Sperrlisten-Verteilungspunkt enthält (z. B. `CertificateRevocationList`).
     - **Admin DN**, **Password:** (nur LDAP) Wenn der CDP-Server keine anonyme Suche für die CRL gestattet, geben Sie Administrator-DN und das Kennwort ein, die zur Authentifizierung am CDP-Server erforderlich sind.
   - **CDP(s) specified in client certificates**

     Wenn das Clientzertifikat nicht alle für den Zugriff auf den Sperrlisten-Verteilungspunkt benötigten Informationen enthält, geben Sie die zusätzlich erforderlichen Informationen an:
     - **CDP Server:** (nur LDAP) Geben Sie den Ort des CDP-Servers ein. Geben Sie bei Verwendung des LDAP-Protokolls die IP-Adresse oder den Hostnamen ein (z. B. `ldap.domain.com`).
     - **CRL Attribute:** (nur LDAP) Geben Sie das LDAP-Atttibut für das Objekt ein, das den Sperrlisten-Verteilungspunkt enthält (z. B. `CertificateRevocationList`).
     - **Admin DN**, **Password:** (nur LDAP) Wenn der CDP-Server keine anonyme Suche für die CRL gestattet, geben Sie Administrator-DN und das Kennwort ein, die zur Authentifizierung am CDP-Server erforderlich sind.

Manually configured CDP

Wenn Sie diese Option auswählen, greift das IVE auf den angegebenen Sperrlisten-Verteilungspunkt zu. Geben Sie den URL des primären Sperrlisten-Verteilungspunktes (CDP) und optional den eines Sicherungs-CDP ein. Verwenden Sie für einen LDAP-Server folgende Syntax: `ldap://Server/BaseDN?attribute?Scope?Filter`. Geben Sie für einen Webserver den vollständigen Pfad zum CRL-Objekt ein. Beispiel:
`http://domain.com/CertEnroll/CompanyName%20CA%20Server.crl`

Wenn der CDP-Server keine anonyme Suche für die CRL gestattet, geben Sie Administrator-DN und das Kennwort ein, die zur Authentifizierung am CDP-Server erforderlich sind. (nur LDAP)

Hinweis: Wenn Sie zum Herunterladen von CDPs eine Methode verwenden und dann eine andere Methode auswählen, löscht das IVE alle Sperrlisten-Verteilungspunkte von der Festplatte, die mit der ersten Methode heruntergeladen wurden.

---

5. Geben Sie im Feld **CRL Download Frequency** an, wie oft das IVE die CRL vom Sperrlisten-Verteilungspunkt herunterladen soll.
6. Wenn Sie die Gültigkeit Ihres Zertifizierungsstellenzertifikats (zusätzlich zu clientseitigen Zertifikaten) anhand der in den vorherigen Schritten angegebenen CRL überprüfen möchten, wählen Sie auf der Seite des Zertifizierungsstellenzertifikats **Verify CA certificate** aus.

   Wichtig:

   - Wenn Sie ein Zwischenzertifikat überprüfen möchten, müssen Sie sicherstellen, dass für alle Zertifizierungsstellenzertifikate, die sich in der Kette über dem Zwischenzertifikat befinden, CRLs verfügbar sind. Beim Überprüfen eines Zertifizierungsstellenzertifikats überprüft das IVE auch alle ausstellenden Zertifizierungsstellen oberhalb des Zertifikats in der Kette.
   - Wenn Sie diese Option auswählen, aber die CRL-Überprüfung nicht aktivieren, überprüft das IVE das Zertifizierungsstellenzertifikat anhand des Sperrlisten-Verteilungspunktes für den Aussteller der Zertifizierungsstelle. Wenn für den Aussteller keine CRL aktiviert ist, schlägt die Benutzerauthentifizierung fehl.
7. Klicken Sie auf **Update Now**, um die CRL manuell vom Sperrlisten-Verteilungspunkt herunterzuladen (optional).
8. Klicken Sie auf **Save Changes**. Das IVE lädt die CRL mit der von Ihnen angegebenen Methode herunter (falls möglich) und zeigt CRL-Überprüfungsdetails an (wie im folgenden Abschnitt beschrieben).

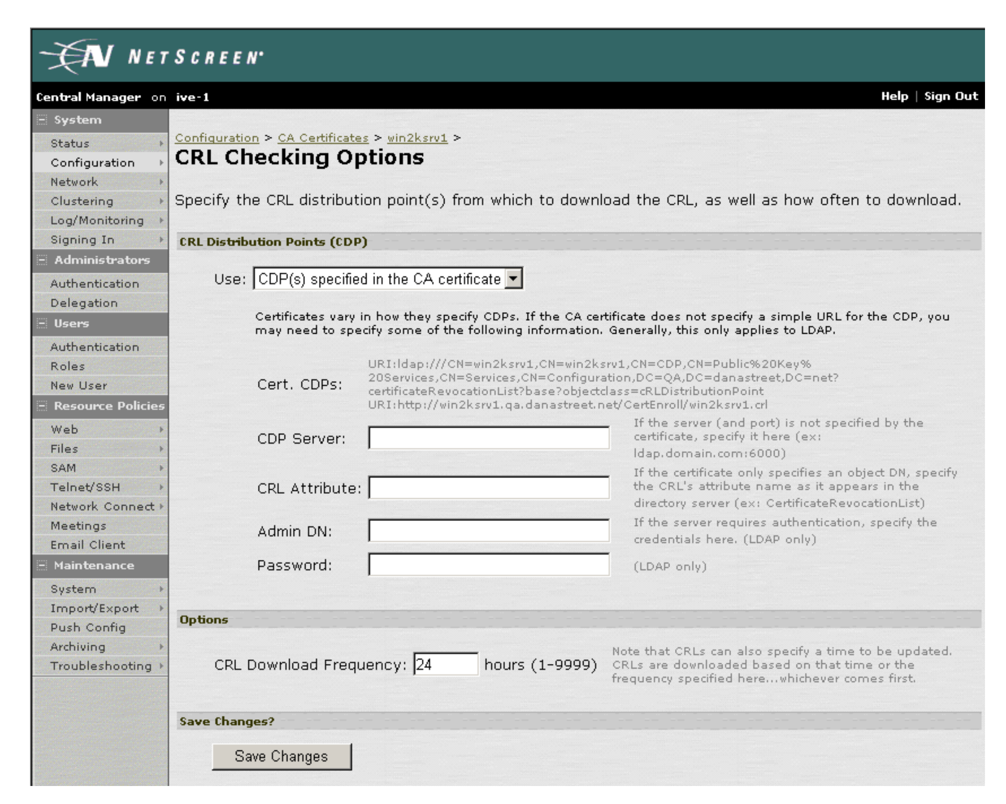


Abbildung 34: **System > Configuration > Certificates > CA Certificates > CRL Checking Options**

☑ Anzeigen von Details für Zertifizierungsstellenzertifikate

Sie können für jedes der auf dem IVE installierten Zertifizierungsstellenzertifikate eine Reihe von Details anzeigen.

So zeigen Sie Details für Zertifizierungsstellenzertifikate an:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > CA Certificate** aus. (**Abbildung 30** auf Seite 192)
2. Klicken Sie auf das Zertifikat, das Sie anzeigen möchten. (**Abbildung 32** auf Seite 193)
3. Verwenden Sie unter **Certificate** den Pfeil neben den folgenden Feldnamen, um Zertifikatdetails anzuzeigen:
   - **Issued To**

     Name und Attribute der Einheit, für die das Zertifikat ausgestellt ist.

- **Issued By**

  Name und Attribute der Einheit, die das Zertifikat ausgestellt hat. Beachten Sie, dass der Wert dieses Feldes entweder dem Inhalt des Feldes **Issued To** (für Stammzertifikate) oder dem des Feldes **Issued To** des nächsten Zertifikats weiter oben in der Kette (für Zwischenzertifikate) entsprechen sollte.

- **Valid Dates**

  Zeitraum der Gültigkeit des Zertifikats. Wenn Ihr Zertifikat abgelaufen ist, finden Sie diesbezügliche Anweisungen unter „Erneuern eines Zertifizierungsstellenzertifikats" auf Seite 193.

- **Details**

  Beinhaltet verschiedene Zertifikatdetails, darunter Version, Seriennummer, Signaturalgorithmus, CRL-Verteilungspunkte, den öffentlichen Schlüssel und dessen Algorithmustyp. Auch wenn das IVE im Feld **Details** einen CRL-Verteilungspunkt anzeigt, überprüft es den Sperrlisten-Verteilungspunkt nur dann, wenn Sie ihn aktivieren. Weitere Informationen finden Sie unter „Aktivieren der CRL-Prüfung" auf Seite 194.

4. Unter **CRL checking for client certificates** können Sie Details der CRL(s) anzeigen, die für dieses Zertifikat aktiviert ist bzw. sind:

   - **Enable**

     Zeigt ein Häkchen an, wenn das IVE zum Verwenden der CRL von diesem Sperrlisten-Verteilungspunkt konfiguriert ist.

   - **CRL Distribution Points**

     Ort des CRL-Verteilungspunktes, anhand dessen die Clientzertifikate überprüft werden. In diesem Feld wird außerdem angezeigt, ob der letzte Versuch zum Herunterladen der CRL vom Sperrlisten-Verteilungspunkt erfolgreich war.

   - **Status**

     Zeigt den Status der CRL („OK", „No CRL", „Expired", „Download in progress"), die Größe der CRL und die Anzahl der in der CRL enthaltenen Sperrungen an.

   - **Last Updated**

     Zeigt die Zeit an, zu der das IVE zuletzt eine CRL von dem angegebenen CRL-Verteilungspunkt heruntergeladen hat. Enthält außerdem eine Verknüpfung, mit der Sie die aktuelle Version der CRL des IVEs speichern können.

   - **Next Update**

     Zeigt die geplante Zeit an, zu der das IVE als nächstes eine CRL von dem angegebenen CRL-Verteilungspunkt herunterladen soll. Beachten Sie, dass sowohl in der CRL als auch auf der CRL-Konfigurationsseite des IVEs ein Intervall zum Herunterladen angegeben ist. Der hier angezeigte Wert ist der kleinere von beiden.

Registerkarte „Certificates > Applet Certificates“

Importieren Sie mithilfe der Registerkarte **System > Configuration > Certificates > Applet Certificate** Codesignaturzertifikate für die Benutzer, wie unter „Appletzertifikate“ auf Seite 72 beschrieben.

☑ Importieren eines Codesignaturzertifikats

So importieren Sie ein Codesignaturzertifikat:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > Applet Certificates** aus.
2. Klicken Sie unter **Applet Signing Certificates** auf **Import Certificates**.
3. Wechseln Sie auf der Seite **Import Certificates** zu den entsprechenden Dateien mit dem Codesignaturzertifikat, geben Sie die Informationen für den Kennwortschlüssel ein, und klicken Sie dann auf **Import**.
4. Geben Sie mithilfe der Einstellungen auf der Registerkarte **Resource Policies > Web > Java > Code Signing** an, welche Ressourcen von dem Appletzertifikat erneut signiert werden sollen.

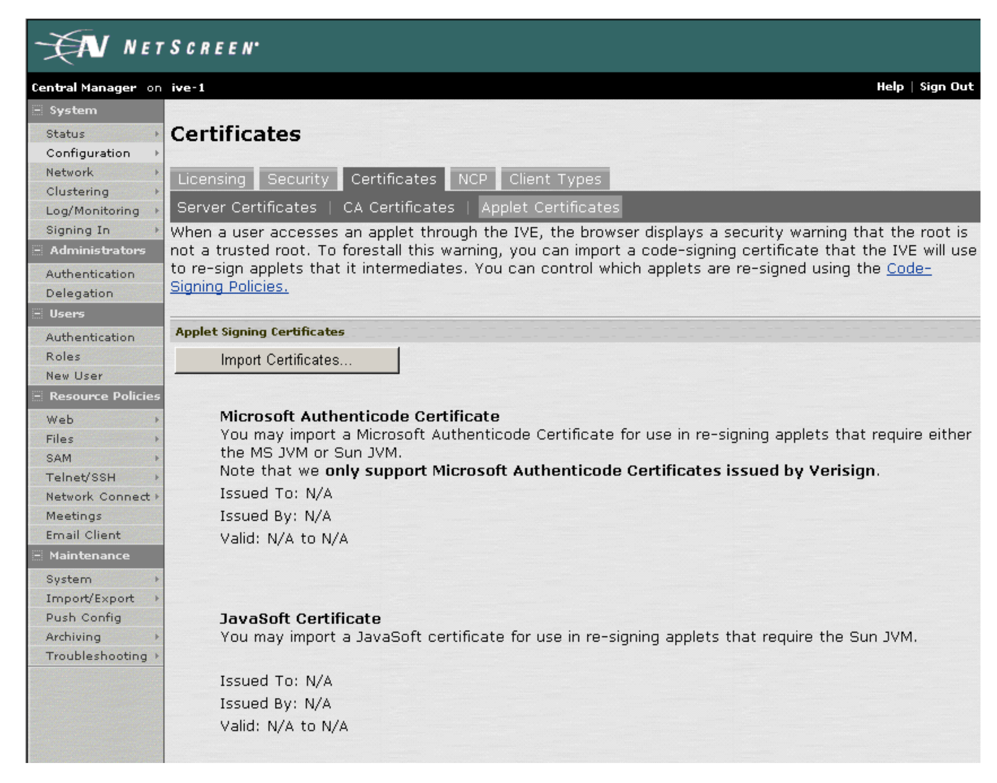


Abbildung 35: **System > Configuration > Certificates > Applet Certificates**

Registerkarte „NCP“

Das Instant Virtual Extranet verwendet die folgenden Typen von internen Protokollen, um zwischen den Server- und Clientanwendungen des IVE zu kommunizieren:

- **NetScreen Communications Protocol (NCP)**

  Das IVE verwendet NCP zum Kommunizieren mit Windows-Clientanwendungen über SSL, darunter der Secure Meeting-Windows-Client, W-SAM und Network Connect.

- **Optimiertes NCP (oNCP)**

  Optimiertes NCP (oNCP) steigert die Durchsatzleistung der Clientanwendungen über NCP erheblich, da es die Protokolleffizienz, Verbindungsverarbeitung und Datenkomprimierung verbessert. oNCP wird nur auf Windows 2000- und Windows XP-Clients unterstützt.

- **Java Communications Protocol (JCP)**

  Das IVE verwendet JCP zum Kommunizieren mit Java-Clientanwendungen, einschließlich von Secure Meeting-Java-Client, J-SAM und Java-Rewriter.

☑ Festlegen von NCP-Optionen für Windows- und Java-Clients

So legen Sie NCP-Optionen fest:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > NCP** aus.
2. (Windows-Clients) Wählen Sie unter **NCP Auto-Select** Folgendes aus:
   - **Auto-select Enabled** (empfohlen) – oNCP wird standardmäßig verwendet. Bei Auswahl dieser Option verwendet das IVE oNCP für den Großteil der Client-/Server-Kommunikation und wechselt dann ggf. zu Standard-NCP. Das IVE wechselt zurück zu NCP, wenn der Benutzer eine nicht unterstützte Plattform verwendet oder wenn die Clientanwendung keine direkte TCP-Verbindung mit dem IVE herstellen kann (z. B. bei Vorhandensein eines Proxys, einer Zeitüberschreitung oder einer Verbindungstrennung).
   - **Auto-select Disabled** – Es wird immer Standard-NCP verwendet. Diese Option wird in erster Linie aus Gründen der Abwärtskompatibilität bereitgestellt.
3. (Java-Clients) Legen Sie unter **Read Connection Timeout** das Zeitlimit für Java-Clients (15-120 Sekunden) fest. Wenn clientseitige Secure Access-Methoden vom IVE keine Daten für das angegebene Intervall erhalten, wird versucht, erneut eine Verbindung mit dem IVE aufzubauen. Beachten Sie, dass sich dieser Wert nicht auf Benutzerinaktivität in Clientanwendungen bezieht.
4. (Windows-Clients) Legen Sie unter **Idle Connection Timeout** das Intervall für das Leerlaufzeitlimit fest. Dieses Leerlaufintervall bestimmt, wie lange das IVE Verbindungen im Leerlauf für clientseitige Secure Access-Methoden für Windows aufrecht erhält.
5. Klicken Sie auf **Save Changes**.

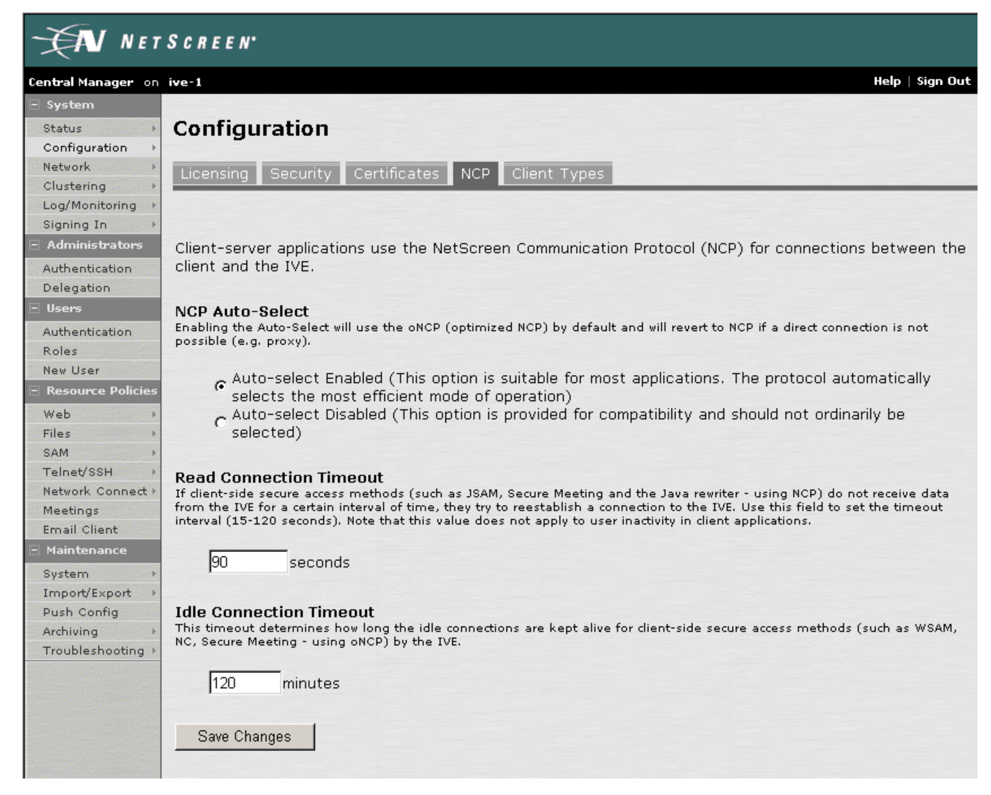


Abbildung 36: System > Configuration > NCP

Registerkarte „Client Types“

Mit der Registerkarte **Client Types** können Sie die Typen von Systemen bestimmen, von denen aus sich die Benutzer anmelden können, und die Typen von HTML-Seiten, die das IVE bei ihrer Anmeldung anzeigt. Weitere Informationen finden Sie unter „Handhelds und PDAs – Übersicht“ auf Seite 96.

☑ Verwalten von Benutzer-Agents

So verwalten Sie Benutzer-Agents:

1. Wählen Sie in der Webkonsole die Optionen **System > Configuration > Client Types** aus.

2. Geben Sie die Benutzer-Agent-Zeichenfolge ein, die dem Betriebssystem oder den Betriebssystemen entspricht, das oder die Sie unterstützen möchten. Sie können Ihre Angabe beliebig weit oder eingeschränkt gestalten. Sie können z. B. die Standardeinstellung des IVE für ***DoCoMo*** verwenden, um sie auf alle DoCoMo-Betriebssysteme anzuwenden, oder Sie können eine Zeichenfolge wie **DoCoMo/1.0/P502i/c10** erstellen, um einen einzelnen Typ von DoCoMo-Betriebssystem anzugeben. Sie können in Ihrer Zeichenfolge die Platzhalter * und ? verwenden.

   Folgende standardmäßige Benutzer-Agent-Zeichenfolgen sind u. a. auf dem IVE vordefiniert:

   - ***DoCoMo* –** Alle DoCoMo-Betriebssysteme (i-mode)
   - ***Windows CE* –** Alle Pocket PC-Betriebssysteme
   - ***Symbian OS* –** Alle Symbian-Betriebssysteme
   - ***SonyEricsson* –** Alle Sony Ericsson-Betriebssysteme
   - * – Alle anderen Betriebssysteme.

   Hinweis: Bei Benutzer-Agent-Zeichenfolgen im IVE muss keine Groß- oder Kleinschreibung beachtet werden.

3. Geben Sie an, welchen HTML-Typ das IVE Benutzern anzeigen soll, die sich von dem im voherigen Schritt angegebenen Betriebssystem anmelden. Folgende Optionen stehen zur Verfügung:

   - **Standard HTML** – Das IVE zeigt alle HTML-Standardfunktionen an, einschließlich Tabellen, Bilder in voller Größe, JavaScript, Java, Frames und Cookies. Ideal für Standardbrowser wie Netscape, Mozilla und Internet Explorer.
   - **Compact HTML** – Das IVE zeigt Compact HTML-kompatible Seiten an, die keine Tabellen, Bilder, Frames, Cookies und kein JavaScript oder Java enthalten. Ideal für iMode-Browser.

     Wichtig: Das IVE schreibt Hyperlinks neu und fügt in den URL die Sitzungs-ID ein, statt Cookies zu verwenden.

   - **Mobile HTML** – Das IVE zeigt HTML-Seiten für mobile Geräte an, die Tabellen, kleine Bilder, JavaScript, Frames, Cookies, aber kein Java enthalten dürfen. Ideal für Pocket PC-Browser.

4. Geben Sie die Reihenfolge an, in der das IVE die Benutzer-Agents auswerten soll. Das IVE wendet die erste Regel in der Liste an, die dem System des Benutzers entspricht. Sie können beispielsweise die folgenden Zuordnungen zwischen Benutzer-Agent-Zeichenfolgen und HTML-Typ in dieser Reihenfolge erstellen:

   1. Benutzer-Agent-Zeichenfolge: ***DoCoMo*** Entspricht: **Compact HTML**
   2. Benutzer-Agent-Zeichenfolge: **DoCoMo/1.0/P502i/c10** Entspricht: **Mobile HTML**

   Wenn sich ein Benutzer von den in der zweiten Zeile angegebenen Betriebssystem anmeldet, zeigt ihm das IVE Compact HTML-Seiten an, und nicht das sicherere HTML für Mobilgeräte, weil seine Benutzer-Agent-Zeichenfolge dem ersten Element in der Liste entspricht.

   Aktivieren Sie zum Anordnen von Zuordnungen in der Liste das Kontrollkästchen neben einem Element, und verschieben Sie es dann mit den nach oben und unten zeigenden Pfeilen zur richtigen Position in der Liste.

5. Aktivieren Sie das Kontrollkästchen **Enable password masking for Compact HTML**, wenn Sie Kennwörter maskieren möchten, die mit iMode oder anderen Geräten eingegeben wurden, die Compact HTML verwenden. (Geräte, die kein Compact HTML verwenden, maskieren Kennwörter immer, unabhängig davon, ob Sie dieses Kontrollkästchen aktivieren oder nicht.) Wenn die Kennwörter Ihrer iMode-Benutzer nicht-numerische Zeichen enthalten, müssen Sie die Kennwortmaskierung deaktivieren, weil iMode-Geräte nur numerische Daten in Standardkennwortfeldern zulassen. Wenn Sie die Maskierung deaktivieren, werden Kennwörter weiterhin sicher übertragen, aber auf der Anzeige des Benutzers nicht verborgen.

6. Klicken Sie auf **Save Changes**.

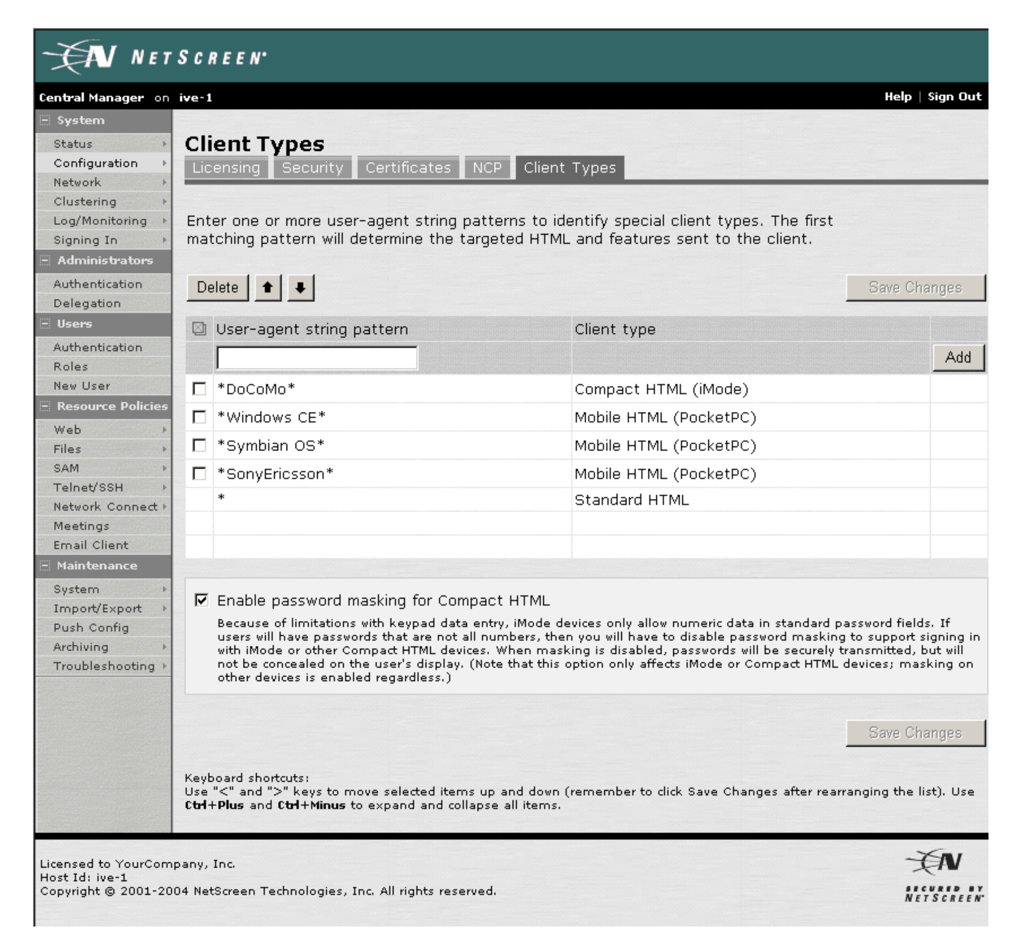


Abbildung 37: **System > Configuration > Client Types**

Konfigurieren der Seite „Network“

Die Seite **System > Network** enthält die folgenden Registerkarten:

Verwenden Sie die Seite **System > Network** für die folgenden Aufgaben:

Registerkarte „Overview“

☑ Konfigurieren allgemeiner Netzwerkeinstellungen

Mithilfe der Seite **Overview** können Sie den Status der internen und externen Ports anzeigen, einen Hostnamen für das IVE angeben und Einstellungen für die DNS-Namensauflösung, den WINS-Server (Windows Internet Naming Service) und den Masterbrowser für das IVE konfigurieren. Beachten Sie, dass die bei der Erstkonfiguration über die serielle Konsole eingegebenen DNS- und WINS-Einstellungen auf dieser Seite angezeigt werden.

So konfigurieren Sie allgemeine Netzwerkeinstellungen:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Overview** aus.
2. Geben Sie unter **Network Identity** den vollständig qualifizierten Hostnamen des IVE ein. Secure Meeting verwendet den angegebenen Hostnamen zum Einfügen der Konferenz-URLs in Benachrichtigungs-E-Mails und für SMTP-Aufrufe (Seite 517). Die Funktion „Pass Through Proxy“ verwendet den angegebenen Hostnamen als Alias für den Hostnamen des Anwendungsservers (Seite 458).

   Hinweis: Wenn die IVE-Appliances in einem Cluster gruppiert sind, wird der von Ihnen angegebene Hostname für die Netzwerkidentität im Cluster synchronisiert. In Clustern mit mehreren Sites empfiehlt es sich jedoch, diese Einstellung zu überschreiben und unterschiedliche Hostnamen für die einzelnen Knoten des Clusters mithilfe der Optionen auf der Seite **System > Clustering** anzugeben.

3. Aktualisieren Sie unter **DNS Name Resolution** die primäre DNS-Adresse, die sekundäre DNS-Adresse und den DNS-Standarddomänennamen für die IVE-Appliance.

   Sie können eine durch Kommas getrennte Liste von DNS-Domänen in diese Felder eingeben. Das IVE durchsucht sie in der Reihenfolge, in der sie aufgelistet sind.

4. Führen Sie unter **Windows Networking** die folgenden Aufgaben aus:
   - Geben Sie den Namen oder die IP-Adresse eines lokalen oder Remote-WINS-Servers (Windows Internet Naming Service) ein, mit dem Sie Namen von Arbeitsstationen und Standorte zu IP-Adressen zuordnen (sofern zutreffend).
   - Klicken Sie auf **Master Browser(s)**, um einen WINS-Server, einen Domänencontroller oder einen anderen Server in der IVE-Domäne auszuwählen, der auf NETBIOS-Aufrufe reagiert und Namen von Arbeitsstationen und Standorte zu IP-Adressen zuordnet (sofern zutreffend). Fügen Sie den Masterbrowser über die Seite **Windows Networking – Specify Master Browser** hinzu.
5. Aktivieren Sie das Kontrollkästchen **Enable network discovery**, damit das IVE freigegebene Windows-Ordner erkennen kann.
6. Klicken Sie auf **Save Changes**.

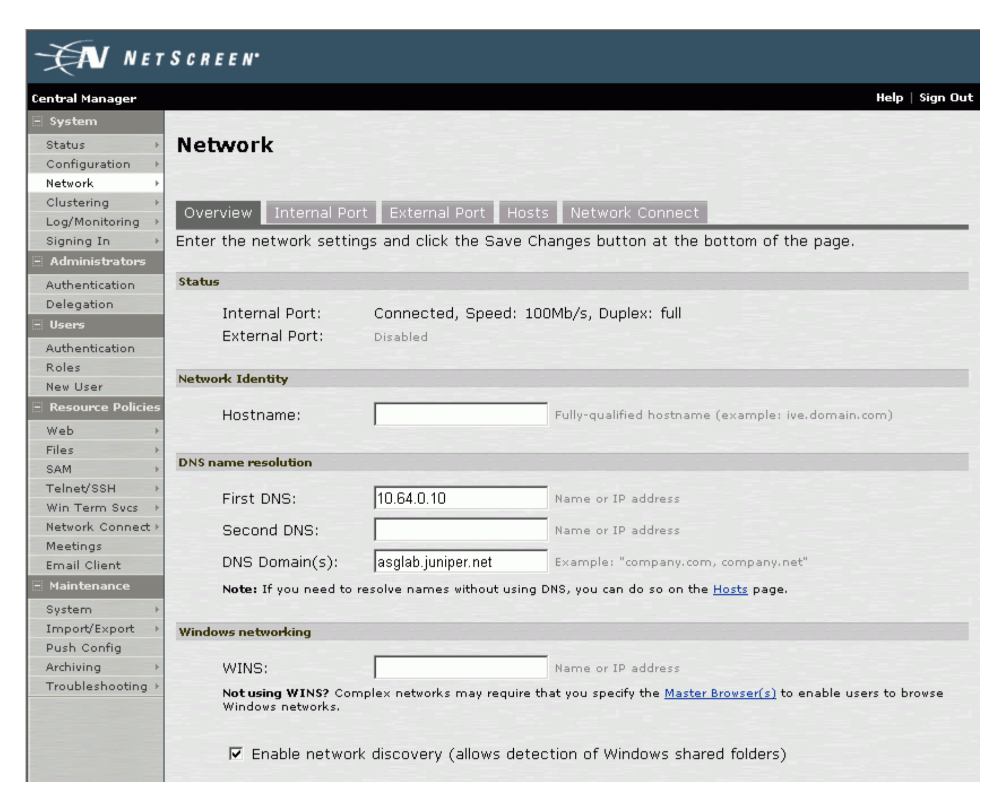


Abbildung 38: **System > Network > Overview**

Registerkarte „Internal Port > Settings“

Wenn Sie die IVE-Appliance installieren, nehmen Sie grundlegende Einstellungen für die LAN-Verbindung über den internen Port der Appliance vor. Über den internen Port werden alle WAN- und LAN-Anforderungen an jede Ressource abgewickelt, d. h. Webbrowserabfragen, Dateiabfragen, Authentifizierung und ausgehende Mailanforderungen. Nachdem Sie das IVE eingerichtet haben, können Sie mithilfe der Registerkarte **System > Network > Internal Port > Settings** die ursprünglichen Einstellungen bei Bedarf aktualisieren. (Sie können die Appliance auch im Dual-Port-Modus bereitstellen, um eingehende Proxy-SSL-Verbindungen für Web und E-Mail an einem externen Port abzufragen, wie unter „Registerkarte „External Port > Settings““ auf Seite 217 beschrieben.)

☑ Ändern von Netzwerkeinstellungen für den internen Port (LAN - Schnittstelle)

Auf der Registerkarte **Internal Port** können Sie die Netzwerkeinstellungen ändern, die Sie während der Ersteinrichtung angegeben haben.

Hinweis: In den meisten Feldern dieser Seite werden bereits die bei der IVE-Installation eingegebenen Einstellungen angezeigt.

So ändern Sie Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle):

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > Settings** aus.
2. Aktualisieren Sie im Abschnitt **Port Information** die Einstellungen für IP-Adresse, Netzmaske, Gateway und Übertragungsrate für die jeweilige IVE-Appliance. Diese Felder enthalten standardmäßig die Einstellungen, die beim ersten IVE-Setup eingegeben wurden.

3. Geben Sie im Feld **ARP Ping Timeout** an, wie lange das IVE höchstens auf Antworten auf ARP-Anforderungen (Address Resolution Protocol) warten soll. Cluster von IVE-Appliances senden ARP-Anforderungen[1] an die Gateways von anderen IVE-Appliances, um zu überprüfen, ob die Kommunikation ordnungsgemäß erfolgt.

Wichtig: Wenn Sie das IVE nicht in einer Clusterumgebung ausführen, wird diese Einstellung nicht verwendet. Wenn die IVEs in einem Cluster gruppiert sind, wird die angegebene Höchstdauer im Cluster synchronisiert. In Clustern mit mehreren Sites können Sie diese Einstellung für die einzelnen Clusterknoten mithilfe der Optionen auf der Seite **System > Clustering** überschreiben. Seien Sie jedoch vorsichtig, wenn Sie diese Einstellung in Aktiv/Passiv-Clustern ändern, da das IVE auch die Einstellung **ARP Ping Timeout** auf der Registerkarte **Internal** als Failover-Zeitgeber für die VIP verwendet.

---

4. Geben Sie im Feld **MTU** eine maximale Übertragungseinheit für die interne Schnittstelle des IVE an.

Hinweis: Es wird empfohlen, die Standardeinstellung (1500) zu verwenden, sofern Sie die Einstellung nicht zwecks Problembehandlung ändern müssen.

---

5. Klicken Sie auf **Save Changes**.

---

1. Das IVE führt beim Versuch, die Kommunikation im Cluster einzurichten, zwei ARP-Anforderungen aus – eine an das Gateway des internen Ports und eine an das Gateway des externen Ports.

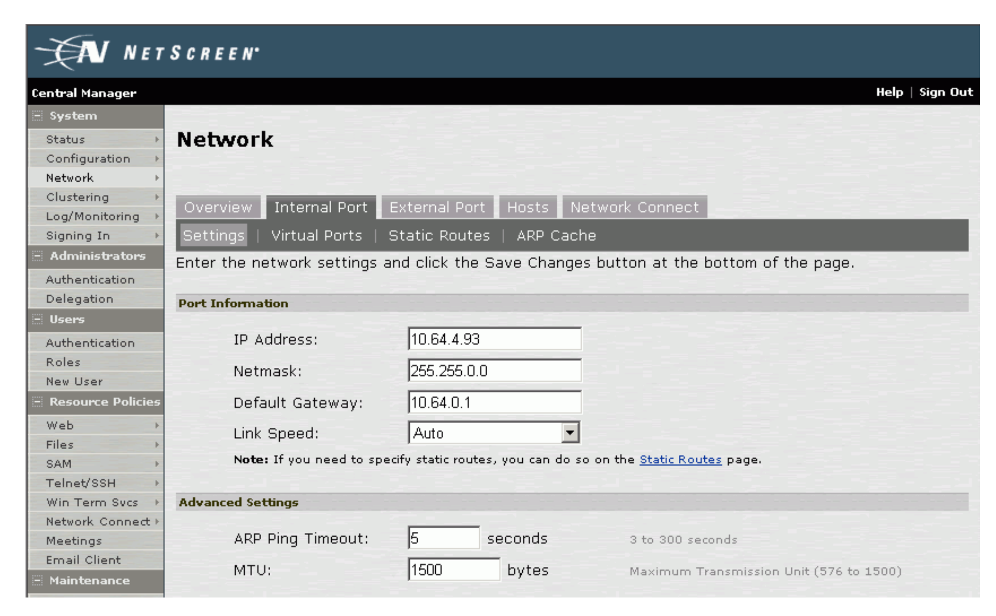


Abbildung 39: **System > Network > Internal Port > Settings**

Registerkarte „Internal Port > Virtual Ports“

☑ Erstellen virtueller Ports für die interne Schnittstelle

Verwenden Sie die Einstellungen auf dieser Registerkarte, um virtuelle Ports für Benutzer (z. B. Mitarbeiter) zu erstellen, die sich innerhalb des internen Netzwerks beim IVE anmelden. Ein ***virtueller Port*** aktiviert einen IP-Alias für einen physischen Port und verwendet alle Netzwerkeinstellungen (mit Ausnahme der IP-Adresse) gemeinsam mit dem internen oder externen Port, der den virtuellen Port hostet. Bei einem ***IP-Alias*** handelt es sich um eine IP-Adresse, die an einen virtuellen Port gebunden ist. (Beachten Sie, dass sich ein IP-Alias von der primären IP-Adresse des IVE unterscheidet, bei der es sich um eine erforderliche IVE-Einstellung handelt, die Sie beim IVE-Initialisierungsvorgang konfigurieren.) Sie können virtuelle Ports in Verbindung mit der Funktion für mehrere Serverzertifikate verwenden, um Benutzern über unterschiedliche IP-Aliase den Zugriff auf dasselbe IVE zu ermöglichen (Seite 185).

Sie können beispielsweise zwei virtuelle Ports für eine einzige Appliance erstellen, wobei Sie dem ersten virtuellen Port die IP-Adresse 10.10.10.1 (`vertrieb.eigenefirma.com`) und dem zweiten virtuellen Port die IP-Adresse 10.10.10.2 (`partner.eigenefirma.com`) zuordnen. Anschließend können Sie jedem dieser virtuellen Ports ein eigenes Zertifikat zuordnen, um sicherzustellen, dass das IVE verschiedene Benutzer über unterschiedliche Zertifikate authentifiziert.

Beachten Sie beim Konfigurieren von virtuellen Ports auf einem in einem Cluster gruppierten IVE, dass alle Knoten im Cluster einige virtuelle Portdaten gemeinsam verwenden. Bei einem Aktiv/Aktiv-Cluster sind zwar die Namen der virtuellen Ports im Cluster gleich, die für die virtuellen Ports definierten IP-Aliase sind jedoch von Knoten zu Knoten unterschiedlich. Bei einem Aktiv/Passiv-Cluster werden sowohl die Namen der virtuellen Ports als auch die IP-Aliase im Cluster gemeinsam verwendet. (Wenn bei einem Aktiv/Passiv-Cluster der zweite Knoten einen Cluster übernimmt, erbt er den IP-Alias des ersten Knotens und aktiviert diesen.)

So erstellen Sie einen virtuellen Port für ein eigenständiges IVE:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > Virtual Ports** aus.
2. Klicken Sie auf **New Port**.
3. Geben Sie einen eindeutigen Namen für den virtuellen Port ein.
4. Geben Sie einen eindeutigen IP-Alias ein, der dem virtuellen Port zugeordnet werden soll. Verwenden Sie keine IP-Adresse, die bereits einem anderen virtuellen Port zugeordnet ist. Beachten Sie, dass der virtuelle Port nicht vom IVE aktiviert wird, wenn Sie keine IP-Adresse eingeben.
5. Klicken Sie auf **Save Changes**.

So erstellen Sie einen virtuellen Port für einen Clusterknoten:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > Virtual Ports** aus.
2. Wählen Sie in der Dropdownliste **Settings for** den Eintrag **Entire cluster** aus, und klicken Sie dann auf **Update**.
3. Klicken Sie auf **New Port**.
4. Geben Sie einen eindeutigen Namen für den virtuellen Port ein, und klicken Sie dann auf **Save Changes**. Das IVE fügt den Namen des virtuellen Ports zur Liste **Virtual Ports** hinzu und bietet Zugriff auf alle Knoten im Cluster.

5. Klicken Sie auf die Verknüpfung zu einem Knoten, um auf die Seite für die IP-Adresskonfiguration zuzugreifen. Geben Sie einen eindeutigen IP-Alias ein, der dem virtuellen Port zugeordnet werden soll. Verwenden Sie keine IP-Adresse, die bereits einem anderen virtuellen Port zugeordnet ist. Beachten Sie, dass der virtuelle Port nicht vom IVE aktiviert wird, wenn Sie keine IP-Adresse eingeben.
6. Klicken Sie auf **Save Changes**. Die Seite **Virtual Ports** wechselt zur Registerkarte für virtuelle Ports zurück. Wählen Sie ggf. in der Dropdownliste **Settings for** erneut den Eintrag **Entire cluster** aus, und wiederholen Sie dann Schritt 5.

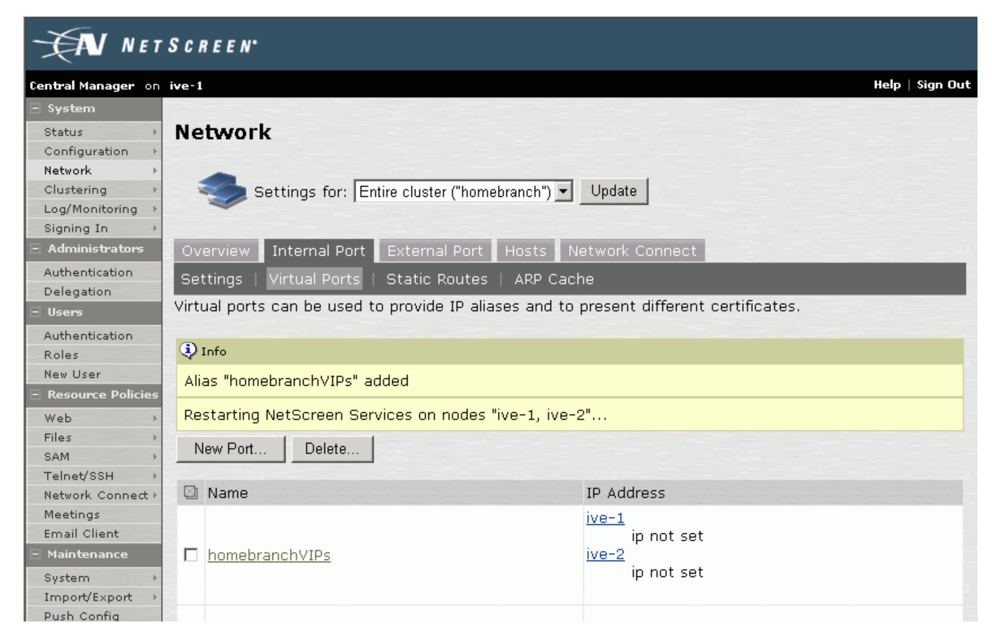


Abbildung 40: **System > Network > Internal Port > Virtual Ports – Entire cluster**

Registerkarte „Internal Port > Static Routes“

☑ Angeben von statischen Routen für den Netzwerkverkehr des internen Ports

Auf der Registerkarte **Static Routes** können Sie Routingtabelleneinträge hinzufügen. Beachten Sie, dass alle Verbindungsanforderungen an interne Ressourcen unabhängig von den Routeneinstellungen über den internen IVE-Port erfolgen. Die Routeneinstellungen des externen Ports werden nur zur Weiterleitung von Paketen verwendet, die Verbindungen zugeordnet sind, die von einem Remoteclient initiiert wurden. Weitere Informationen finden Sie unter „Registerkarte „External Port > Settings““ auf Seite 217.

So geben Sie statische Routen an:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > Static Routes** aus.
2. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Add**.

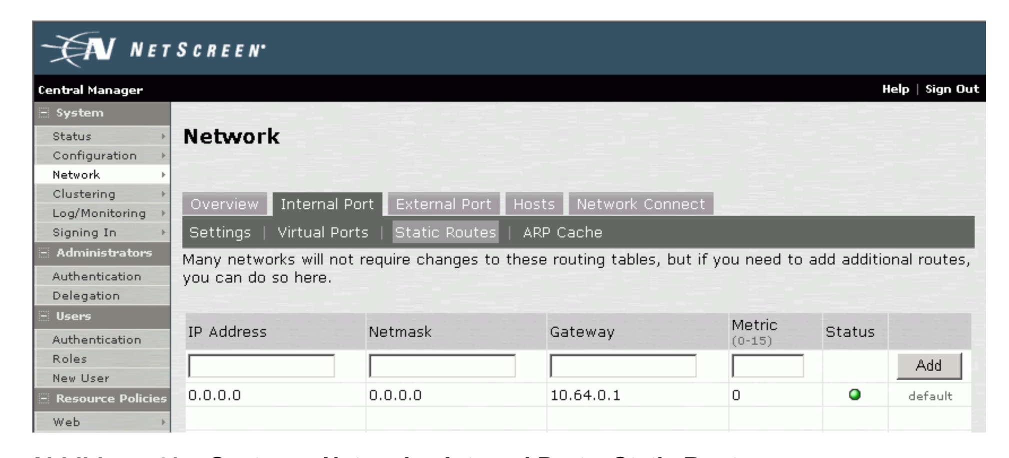


Abbildung 41: **System > Network > Internal Port > Static Routes**

Registerkarte „Internal Port > ARP Cache“

Mithilfe der ARP-Zwischenspeicherung können Sie die physische Adresse (MAC-Adresse) eines Netzwerkgeräts (z. B. eines Routers oder Back-End-Anwendungsservers) ermitteln, das eine Verbindung mit dem IVE herstellt. Verwenden Sie die Registerkarte **ARP Cache**, um folgende Typen von ARP-Einträgen (Address Resolution Protocol) zu verwalten:

- **Statische Einträge**

  Sie können dem Cache, der der IP- und MAC-Adresse zugeordnet ist, einen statischen ARP-Eintrag hinzufügen. Das IVE speichert statische Einträge während eines Neustarts und reaktiviert sie nach dem Neustart. Statische Einträge sind immer auf dem IVE verfügbar.

- **Dynamische Einträge**

  Das Netzwerk „erlernt“ dynamische ARP-Einträge während der regulären Verwendung und Interaktion mit anderen Netzwerkgeräten. Die dynamischen Einträge werden vom IVE bis zu 20 Minuten zwischengespeichert und bei einem Neustart gelöscht. Sie haben auch die Möglichkeit, die dynamischen Einträge manuell zu löschen.

Sie können statische und dynamische Einträge aus dem ARP-Cache anzeigen und löschen sowie statische Einträge hinzufügen. Wenn Sie über einen Cluster von IVEs verfügen, sollten Sie beachten, dass ARP-Cacheinformationen knotenspezifisch sind.

☑ Hinzufügen eines statischen Eintrags

So fügen Sie einen statischen Eintrag hinzu:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > ARP Cache** aus.
2. Nehmen Sie im oberen Bereich der Tabelle in den dafür vorgesehenen Feldern **IP Address** und **Physical Address** die entsprechenden Eingaben vor.

   Hinweis: Beachten Sie Folgendes: Wenn Sie einen Eintrag mit einer bereits vorhandenen IP-Adresse hinzufügen, überschreibt das IVE den vorhandenen Eintrag mit dem neuen Eintrag. Außerdem sollten Sie beachten, dass das IVE nicht die Gültigkeit von MAC-Adressen überprüft.

3. Klicken Sie auf **Add**.

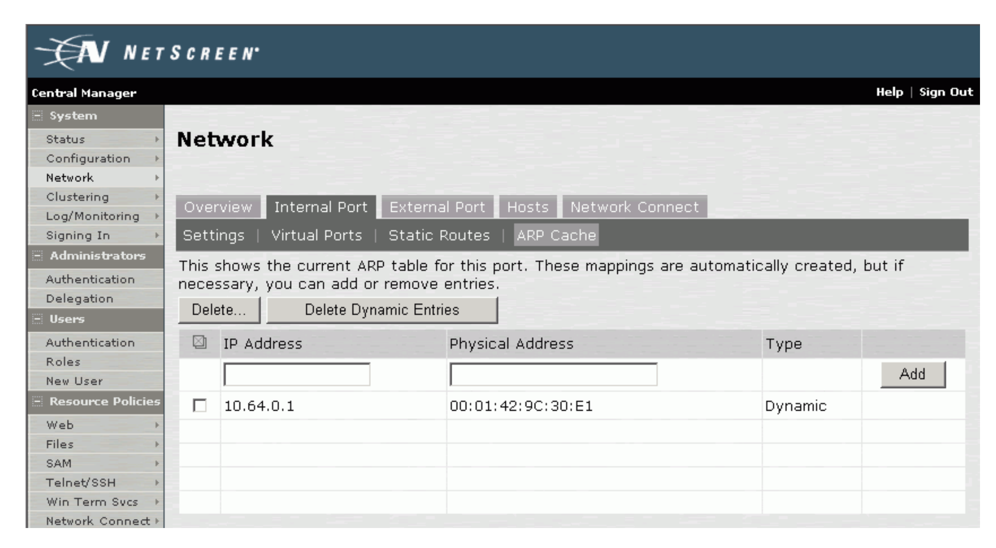


Abbildung 42: **System > Network > Internal Port > ARP Cache**

Registerkarte „External Port > Settings“

Die externe DMZ-Schnittstelle (Demilitarized Zone) fragt nur Anforderungen von Benutzern ab, die am IVE angemeldet sind, und leitet nur deren Anforderungen weiter. Vor dem Senden eines Pakets ermittelt das IVE, ob das Paket einer TCP-Verbindung zugeordnet ist, die von einem Benutzer über die externe Schnittstelle initiiert wurde. Ist dies der Fall, sendet das IVE das Paket an die externe Schnittstelle. Alle übrigen Pakete werden an die interne Schnittstelle gesendet. Die für jede Schnittstelle festgelegten Routen werden verwendet, nachdem das IVE ermittelt hat, ob die interne oder die externe Schnittstelle zu verwenden ist. Das IVE leitet keine Anforderungen von der externen Schnittstelle ein, und diese Schnittstelle akzeptiert keine anderen Verbindungen (mit Ausnahme von Ping- und Tracerouteverbindungen). Alle Anforderungen an eine beliebige Ressource werden von der internen Schnittstelle ausgegeben. (Weitere Informationen finden Sie unter „Registerkarte „Internal Port > Settings““ auf Seite 210.)

☑ Aktivieren des externen Ports (DMZ-Schnittstelle)

Auf der Registerkarte **External Port** können Sie die DMZ-Funktion aktivieren. Beachten Sie Folgendes: Wenn Sie die DMZ-Funktion aktivieren, können sich Administratoren standardmäßig nicht mehr von einem externen Standort aus anmelden. Sie können den externen Port für Administratoren auf der Registerkarte **Administrators > Authentication > Authentication Policy > Source IP** öffnen.

So aktivieren Sie den externen Port:

1. Wählen Sie in der Webkonsole die Optionen **System > Network** > **External Port > Settings** aus.
2. Aktivieren Sie unter **Use External Port** die Option **Enabled**.
3. Geben Sie im Abschnitt **Port Information** die IP-Adresse, Netzmaske, das Gateway und die Übertragungsrate für den externen Port des IVE ein. In der Regel empfiehlt es sich, die Einstellungen der Seite **Internal Port > Settings** zu übernehmen und dann die Informationen zum internen Port in eine lokale IP-Adresse und Netzmaske sowie ein lokales Gateway zu ändern.
4. Geben Sie im Feld **ARP Ping Timeout** an, wie lange das IVE höchstens auf Antworten auf ARP-Anforderungen (Address Resolution Protocol) warten soll. Cluster von IVE-Appliances senden ARP-Anforderungen[1] an die Gateways von anderen IVE-Appliances, um zu überprüfen, ob die Kommunikation ordnungsgemäß erfolgt.

   Hinweis: Wenn die IVEs in einem Cluster gruppiert sind, wird die angegebene Höchstdauer im Cluster synchronisiert. In Clustern mit mehreren Sites können Sie diese Einstellung für die einzelnen Knoten mithilfe der Optionen auf der Seite **System > Clustering** überschreiben. Wenn Sie das IVE nicht in einer Clusterumgebung ausführen, wird die Einstellung für **ARP Ping Timeout** nicht verwendet.

5. Geben Sie im Feld **MTU** eine maximale Übertragungseinheit für die externe Schnittstelle des IVE an.

   Hinweis: Es wird empfohlen, die Standardeinstellung (1500) zu verwenden, sofern Sie die Einstellung nicht zwecks Problembehandlung ändern müssen.

6. Klicken Sie auf **Save Changes**.

1. Das IVE führt beim Versuch, die Kommunikation im Cluster einzurichten, zwei ARP-Anforderungen aus – eine an das Gateway des internen Ports und eine an das Gateway des externen Ports.

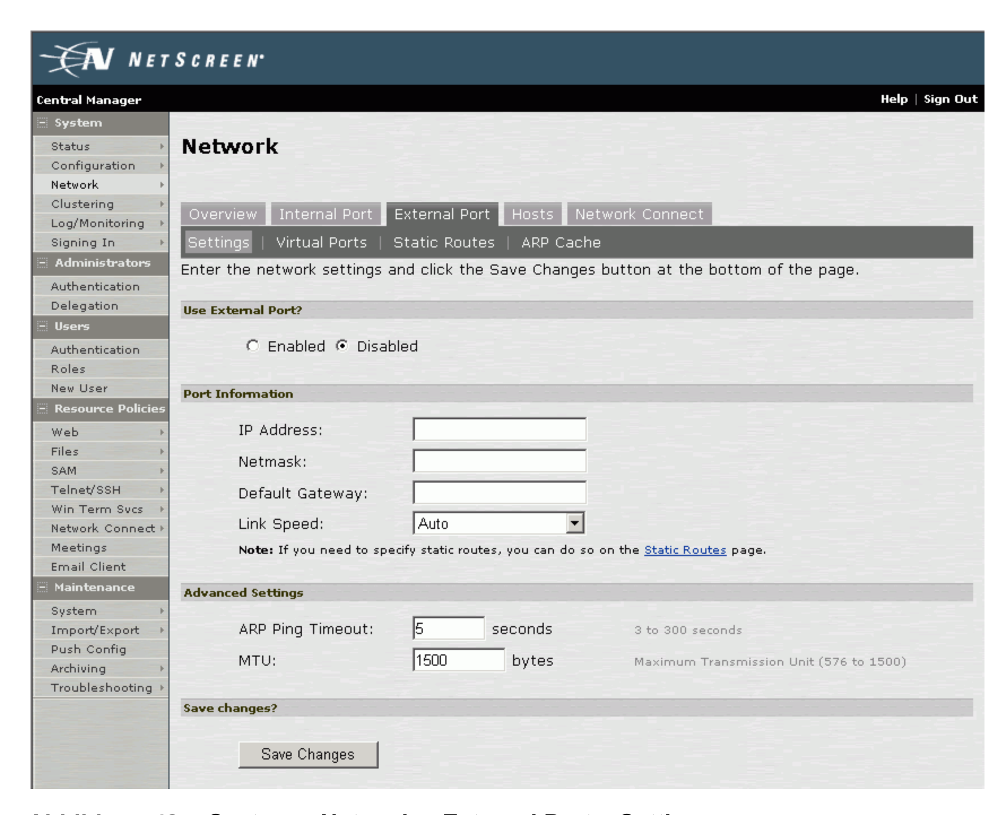


Abbildung 43: **System > Network > External Port > Settings**

Registerkarte „External Port > Virtual Ports“

☑ Erstellen virtueller Ports für den externen Port

Verwenden Sie die Einstellungen auf dieser Registerkarte, um virtuelle Ports für Benutzer (z. B. Kunden und Partner) zu erstellen, die sich außerhalb Ihres internen Netzwerks beim IVE anmelden. Dies wird unter „Registerkarte „Internal Port > Virtual Ports““ auf Seite 212 erläutert.

So erstellen Sie einen virtuellen Port für ein eigenständiges IVE:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > External Port > Virtual Ports** aus.
2. Klicken Sie auf **New Port**.

3. Geben Sie einen eindeutigen Namen für den virtuellen Port ein.
4. Geben Sie einen eindeutigen IP-Alias ein, der dem virtuellen Port zugeordnet werden soll. Verwenden Sie keine IP-Adresse, die bereits einem anderen virtuellen Port zugeordnet ist. Beachten Sie, dass der virtuelle Port nicht vom IVE aktiviert wird, wenn Sie keine IP-Adresse eingeben.
5. Klicken Sie auf **Save Changes**.
6. Verwenden Sie die Einstellungen auf der Registerkarte **System > Configuration > Certificates > Server Certificates**, um dem virtuellen Port ein Serverzertifikat zuzuordnen (Seite 185).

So erstellen Sie einen virtuellen Port für einen Clusterknoten:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > External Port > Virtual Ports** aus.
2. Wählen Sie in der Dropdownliste **Settings for** den Eintrag **Entire cluster** aus, und klicken Sie dann auf **Update**.
3. Klicken Sie auf **New Port**.
4. Geben Sie einen eindeutigen Namen für den virtuellen Port ein, und klicken Sie dann auf **Save Changes**. Das IVE fügt den Namen des virtuellen Ports zur Liste **Virtual Ports** hinzu und bietet Zugriff auf alle Knoten im Cluster.
5. Klicken Sie auf die Verknüpfung zu einem Knoten, um auf die Seite für die IP-Adresskonfiguration zuzugreifen. Geben Sie einen eindeutigen IP-Alias ein, der dem virtuellen Port zugeordnet werden soll. Verwenden Sie keine IP-Adresse, die bereits einem anderen virtuellen Port zugeordnet ist. Beachten Sie, dass der virtuelle Port nicht vom IVE aktiviert wird, wenn Sie keine IP-Adresse eingeben.
6. Klicken Sie auf **Save Changes**. Die Seite **Virtual Ports** wechselt zur Registerkarte für virtuelle Ports zurück. Wählen Sie ggf. in der Dropdownliste **Settings for** erneut den Eintrag **Entire cluster** aus, und wiederholen Sie dann Schritt 5.

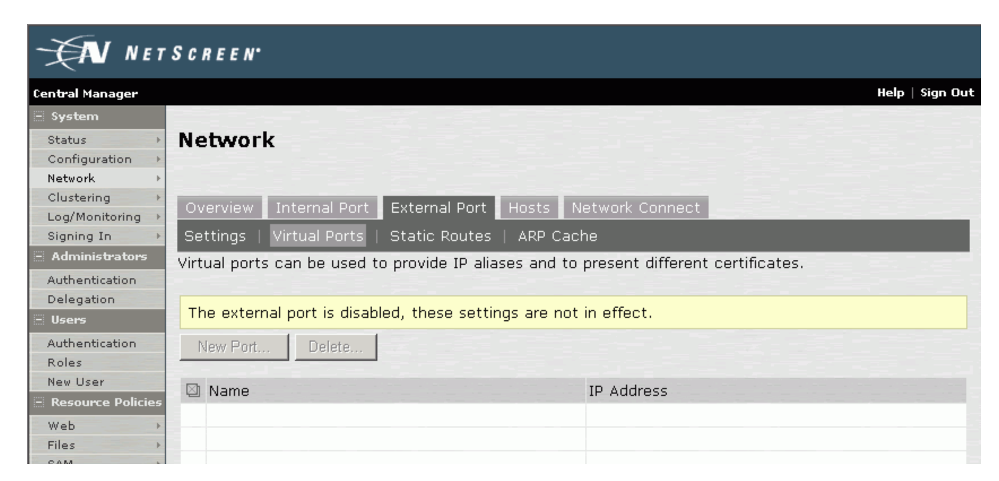


Abbildung 44: **System > Network > External Port > Virtual Ports**

Registerkarte „External Port > Static Routes“

☑ Angeben von statischen Routen für den Netzwerkverkehr des externen Ports

Auf der Registerkarte **Static Routes** können Sie Routingtabelleneinträge hinzufügen. Beachten Sie, dass alle Verbindungsanforderungen an interne Ressourcen unabhängig von den Routeneinstellungen über den internen IVE-Port erfolgen. Die Routeneinstellungen des externen Ports werden nur zur Weiterleitung von Paketen verwendet, die Verbindungen zugeordnet sind, die von einem Remoteclient initiiert wurden. Weitere Informationen finden Sie unter „Registerkarte „External Port > Settings““ auf Seite 217.

So geben Sie statische Routen an:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Internal Port > Static Routes** aus.
2. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Add**.

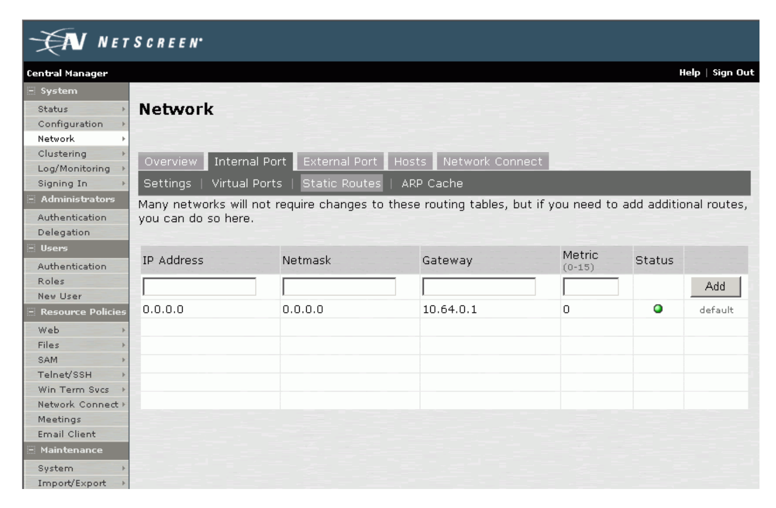


Abbildung 45: System > Network > Internal Port > Static Routes

Registerkarte „External Port > ARP Cache"

Mithilfe der ARP-Zwischenspeicherung können Sie die physische Adresse (MAC-Adresse) eines Netzwerkgeräts (z. B. eines Routers oder Back-End-Anwendungsservers) ermitteln, das eine Verbindung mit dem IVE herstellt. Verwenden Sie die Registerkarte **ARP Cache**, um folgende Typen von ARP-Einträgen (Address Resolution Protocol) zu verwalten:

- **Statische Einträge**

  Sie können dem Cache, der der IP- und MAC-Adresse zugeordnet ist, einen statischen ARP-Eintrag hinzufügen. Das IVE speichert statische Einträge während eines Neustarts und reaktiviert sie nach dem Neustart. Statische Einträge sind immer auf dem IVE verfügbar.

- **Dynamische Einträge**

  Das Netzwerk „erlernt" dynamische ARP-Einträge während der regulären Verwendung und Interaktion mit anderen Netzwerkgeräten. Die dynamischen Einträge werden vom IVE bis zu 20 Minuten zwischengespeichert und bei einem Neustart gelöscht. Sie haben auch die Möglichkeit, die dynamischen Einträge manuell zu löschen.

Sie können statische und dynamische Einträge aus dem ARP-Cache anzeigen und löschen sowie statische Einträge hinzufügen. Wenn Sie über einen Cluster von IVEs verfügen, sollten Sie beachten, dass ARP-Cacheinformationen knotenspezifisch sind.

☑ Hinzufügen eines statischen Eintrags

So fügen Sie einen statischen Eintrag hinzu:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > External Port > ARP Cache** aus.
2. Nehmen Sie im oberen Bereich der Tabelle in den dafür vorgesehenen Feldern **IP Address** und **Physical Address** die entsprechenden Eingaben vor.

   Hinweis: Beachten Sie Folgendes: Wenn Sie einen Eintrag mit einer bereits vorhandenen IP-Adresse hinzufügen, überschreibt das IVE den vorhandenen Eintrag mit dem neuen Eintrag. Außerdem sollten Sie beachten, dass das IVE nicht die Gültigkeit von MAC-Adressen überprüft.

3. Klicken Sie auf **Add**.

Registerkarte „Hosts“

☑ Angeben von Hostnamen, die vom IVE lokal aufgelöst werden sollen

Auf der Registerkarte **Hosts** können Sie Hostnamen angeben, die vom IVE lokal zu IP-Adressen aufgelöst werden können. Diese Funktion bietet sich in folgenden Fällen an:

- Das IVE kann nicht auf den DNS-Server zugreifen
- Im LAN wird über WINS auf Server zugegriffen
- Die Sicherheitsrichtlinien Ihres Unternehmens lassen die Auflistung interner Server auf einem externen DNS nicht zu oder erfordern die Maskierung interner Hostnamen

Wenn Sie auf der Registerkarte **System > Network Settings > Hosts** eines Clusters Hostnamenzuordnungen eingeben, werden die Einstellungen für die anderen Knoten übernommen.

So geben Sie Hostnamen an, die das IVE lokal auflösen soll:

1. Wählen Sie in der Webkonsole die Registerkarte **System > Network > Hosts** aus.
2. Geben Sie eine IP-Adresse, eine durch Kommas getrennte Liste von Hostnamen, die zu der IP-Adresse aufgelöst werden, und bei Bedarf einen Kommentar von höchstens 200 Wörtern ein, und klicken Sie dann auf **Add**.

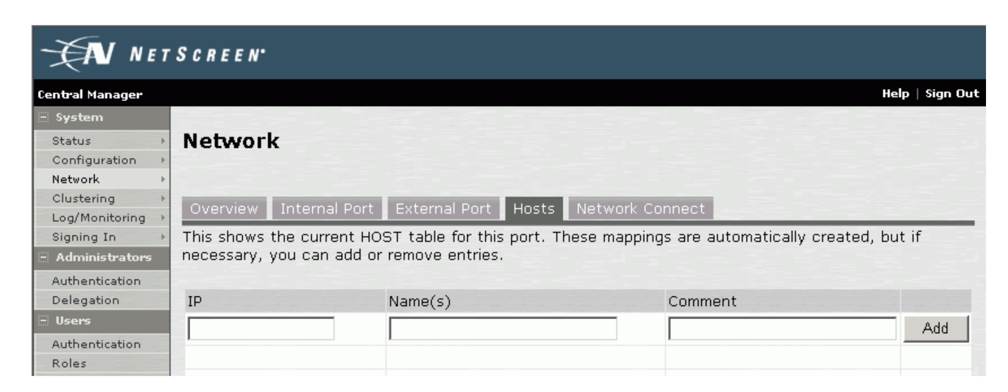


Abbildung 46: System > Network > Hosts

Registerkarte „Network Connect“

Verwenden Sie die Registerkarte **Network Connect**, um das Network Connect-Installationsprogramm herunterzuladen und IP-Filter für das IVE anzugeben, die auf Network Connect-IP-Pools angewendet werden sollen. Weitere Informationen finden Sie unter „Network Connect – Übersicht“ auf Seite 107.

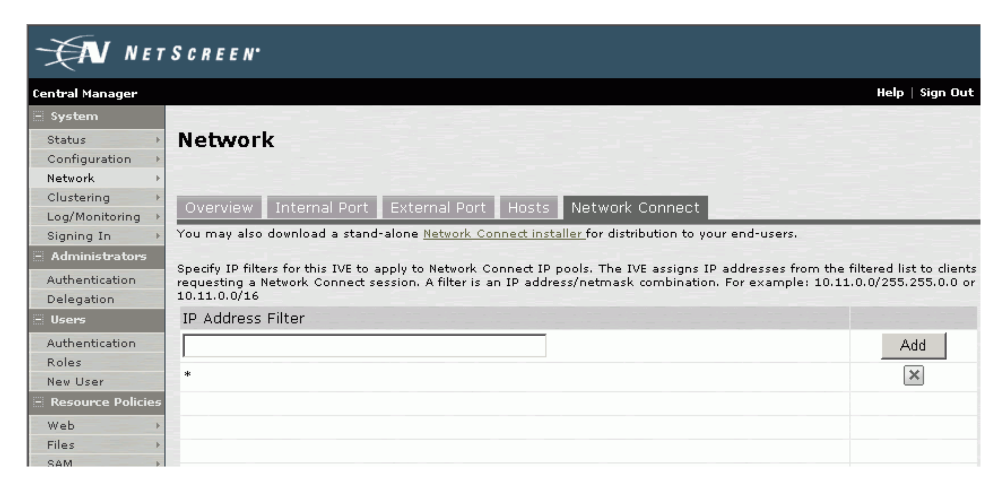


Abbildung 47: **System > Network > Network Connect**

☑ Herunterladen des Network Connect-Installationsprogramms

Sie können die Anwendung Network Connect als ausführbare Windows-Datei herunterladen, die Ihnen folgende Möglichkeiten bietet:

- Verteilen der Datei auf mehrere Clientcomputer mithilfe von Softwareverteilungstools. Mit dieser Option können Sie Network Connect auf Clientcomputern installieren, deren Benutzer nicht über die zum Installieren von Network Connecterforderlichen Administratorrechte verfügen.
- Bereitstellen der ausführbaren Datei in einem sicheren Repository, damit Benutzer die richtige Version herunterladen und installieren können.

Mit diesen Optionen können Sie steuern, welche Version von Network Connect auf Clientcomputern ausgeführt wird.

So laden Sie das Network Connect-Installationsprogramm herunter:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Network Connect** aus.
2. Klicken Sie unter **Policies** auf die Verknüpfung des **Network Connect**-Installationsprogramms, um die ausführbare Datei von Network Connect vom IVE herunterzuladen.

☑ Angeben von IP-Filtern für das IVE, die auf Network Connect-IP-Pools angewendet werden sollen

Knoten in einem Cluster nutzen die Konfigurationsinformationen gemeinsam, d. h., dass IVEs in verschiedenen Netzwerken einen IP-Pool gemeinsam verwenden. Da jeder IVE-Knoten die Clientanforderung zum Starten der Network Connect-Sitzung empfangen kann, müssen Sie einen IP-Filter für den Knoten angeben, der nur die für diesen Knoten verfügbaren Netzwerkadressen herausfiltert. Wenn der Clusterknoten eine Anforderung zum Erstellen einer Network Connect-Sitzung empfängt, weist er aus dem gefilterten IP-Pool die zwei IP-Adressen für die Sitzung zu.

So fügen Sie der Network Connect-Filterliste eine IP-Adresse hinzu:

1. Wählen Sie in der Webkonsole die Optionen **System > Network > Network Connect** aus.
2. Geben Sie eine Kombination aus IP-Adresse und Netzmaske an, und klicken Sie dann auf **Add**. Das IVE wendet die auf dieser Seite angegebenen Filter auf die Ressourcenrichtlinien für Network Connect-IP-Pools an, die auf eine Anforderung eines Benutzers angewendet werden.

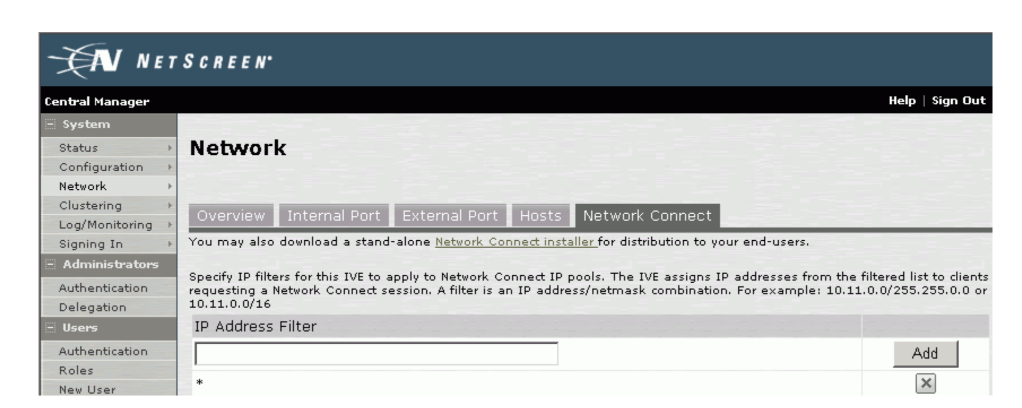


Abbildung 48: System > Network > Network Connect

Konfigurieren der Seite „Clustering“

Vor dem Erstellen eines Clusters müssen Sie sicherstellen, dass es sich bei allen vorgesehenen IVE-Knoten um die gleiche Hardwareplattform handelt (beispielsweise alle Access Series 3000-Geräte), und dass auf allen Knoten die gleiche Dienstpaketversion ausgeführt wird. Wenn Sie Juniper Networks NetScreen-SA Central Manager erworben haben, können Sie über das IVE, das mit der neuesten Betriebssystemversion ausgeführt wird, einen Cluster erstellen und dann mit der Funktion zum Aktualisieren und Einfügen zusätzliche Knoten hinzufügen. Wenn Sie mit dieser Funktion einen Knoten zu einem Cluster hinzufügen, aktualisiert der erste IVE-Knoten den einzufügenden Knoten mit dem aktuelleren Dienstpaket. Diese Funktion ist nur verfügbar, wenn alle IVEs Version 4.0 oder höher des Betriebssystems ausführen.

Weitere Informationen finden Sie unter „Cluster – Übersicht“ auf Seite 79.

Wichtig: Wir empfehlen, einen Cluster zunächst in einer Stagingumgebung bereitzustellen und erst zu einer Produktionsumgebung zu wechseln, nachdem Sie den Authentifizierungsbereich, die Benutzerrolle und Ressourcenrichtlinienkonfiguration sowie die Anwendungen, die die Endbenutzer möglicherweise verwenden, getestet haben.

Wenn ein IVE nicht Teil eines Clusters ist, enthält seine Seite **System > Clustering** die folgenden beiden Registerkarten:

Mit den Registerkarten **Create**[1] und **Join** können Sie Folgendes durchführen:

Hinweis: Informationen über das Beitreten eines nicht initialisierten IVE zu einem Cluster finden Sie unter „Hinzufügen eines IVE zu einem Cluster über die serielle Konsole“ auf Seite 245.

1. Die Registerkarte **Create** wird nur auf IVEs angezeigt, die nicht über die Clusterlizenz verfügen.

Wenn ein IVE Teil eines Clusters ist, enthält seine Seite **System > Clustering** die folgenden beiden Registerkarten:

Mit den Registerkarten **Status** und **Properties** können Sie Folgendes durchführen:

Registerkarte „Create“

Verwenden Sie die Registerkarte **Create**, um einen Cluster zu definieren und zu initialisieren. Das Definieren eines Clusters besteht im Angeben eines Namens und eines Kennwortes für den Cluster sowie eines Namens für das erste Mitglied des Clusters. Nach dem Erstellen des Clusters wird anstelle der Registerkarte **Create** die Registerkarte **Status** angezeigt. Mit dieser Registerkarte können Sie zusätzliche IVEs zum Cluster hinzufügen. Fügen Sie dann über die Registerkarte **Clustering > Join** der einzelnen IVEs diese IVEs zum Cluster hinzu. (Wenn Sie einem Cluster ein nicht initialisiertes IVE hinzufügen möchten, finden Sie Informationen dazu unter „Hinzufügen eines IVE zu einem Cluster über die serielle Konsole“ auf Seite 245.)

Hinweis: Zum Erstellen eines Clusters müssen Sie vorher eine Clusterlizenz eingeben.

☑ Definieren und Initialisieren eines Clusters

Wenn Sie momentan eigenständige IVEs ausführen, die Sie zu einem Cluster zusammenfassen möchten, sollten Sie vor dem Erstellen eines Clusters zunächst die System- und Benutzereinstellungen auf einem Computer konfigurieren. Erstellen Sie anschließend auf dem gleichen IVE den Cluster. Dieses IVE wird dem Cluster im Rahmen des Erstellungsvorgangs hinzugefügt. Wenn dem Cluster weitere IVEs beitreten, gibt dieses IVE seine Konfiguration an die neuen Clustermitglieder weiter.

So definieren und initialisieren Sie einen Cluster:

1. Konfigurieren Sie ein IVE mit den gewünschten System-, Benutzer-, Ressourcen- und Anwendungseinstellungen.
2. Wählen Sie in der Webkonsole des konfigurierten IVE die Registerkarte **System > Configuration > Licensing** aus, und geben Sie Ihren Lizenzcode ein, um die Clusterfunktion und die Registerkarte **Clustering > Create** zu aktivieren.
3. Wählen Sie **System > Clustering > Create** aus, geben Sie einen Namen und ein Kennwort für den Cluster sowie einen Namen für den Computer ein, z. B. `ive-1`.

   Hinweis: Wenn Sie weitere IVEs konfigurieren, die dem Cluster hinzugefügt werden sollen, müssen Sie das Kennwort erneut eingeben. Alle IVEs in dem Cluster verwenden dieses Kennwort für die Kommunikation.

4. Klicken Sie auf **Create Cluster**. Klicken Sie auf **Create**, wenn Sie aufgefordert werden, die Erstellung des neuen Clusters zu bestätigen. Nachdem das IVE den Cluster initialisiert hat, werden auf der Seite **Clustering** die Registerkarten **Status** und **Properties** angezeigt. Mit der Registerkarte **Status** können Sie weitere Clustermitglieder angeben (Seite 236), bevor Sie versuchen, ein weiteres IVE zum neuen Cluster hinzuzufügen.

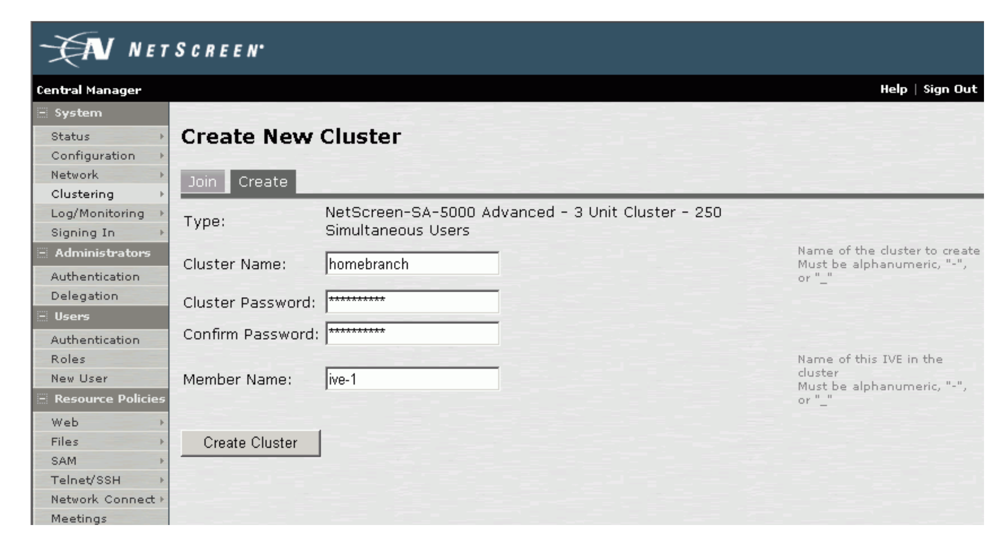


Abbildung 49: **System > Clustering > Create – Startseite**

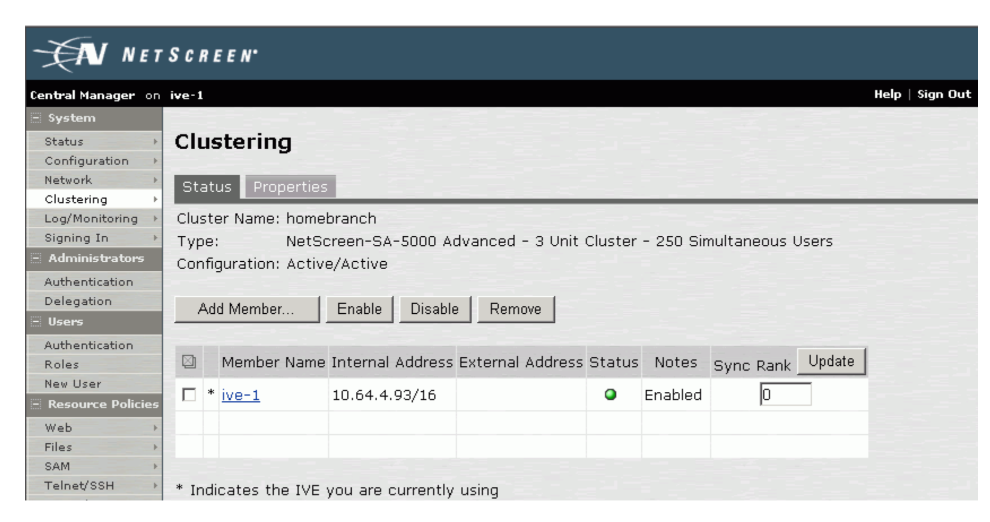


Abbildung 50: System > Clustering > Status – Nach dem Erstellen eines Clusters
Die Abbildung zeigt die Seite „Clustering" nach der Erstellung eines Clusters. Das IVE, auf dem Sie den Cluster definieren, wird zum ersten Clustermitglied.

Registerkarte „Join“

Mit der Registerkarte **Join** können Sie ein IVE zu einem vorhandenen Cluster hinzufügen. Die Art des Beitretens eines IVE zu einem Cluster hängt davon ab, ob das IVE konfiguriert oder nicht initialisiert (noch im Werkzustand) ist. Für ein IVE im Werkzustand empfehlen wir das Verfahren über die serielle Konsole (Seite 245), da für den Beitritt des IVE zum Cluster nur wenige Informationen eingegeben werden müssen.

In einer Access Series FIPS-Umgebung müssen Sie zum Hinzufügen eines IVE zu einem Cluster die **Webkonsole** verwenden. Darüber hinaus müssen Sie über physischen Zugang zu folgenden Einheiten verfügen:

- Die Kryptographiemodule, die an den Frontplatten der IVE-Appliances der Custermitglieder angebracht sind
- Einen Smartcardleser
- Eine Administratorkarte, die mit der Security World des aktiven Clustermitglieds vorinitialisiert ist

☑ Hinzufügen eines IVEs zu einem Cluster über dessen Webkonsole

Bevor Sie ein IVE zu einem Cluster hinzufügen können (entweder über die Web- oder die serielle Konsole), müssen Sie dem Cluster dessen Identität mitteilen. Anweisungen zur Angabe eines IVE, dass einem Cluster hinzugefügt werden soll, finden Sie unter „Angeben eines IVE zum Hinzufügen zu einem Cluster“ auf Seite 236. Wenn ein IVE nicht über eine Clusterlizenz verfügt, weist es nur eine Registerkarte **Clustering > Join** auf.

Wichtig: Wenn Sie ein IVE, das gegenwärtig als eigenständiges Gerät ausgeführt wird, über seine **Webkonsole** zu einem Cluster hinzufügen möchten, muss dasselbe oder ein älteres Dienstpaket auf der gleichen Hardwareplattform wie bei den anderen Mitgliedern ausgeführt werden.

So fügen Sie ein IVE über die Webkonsole einem Cluster hinzu:

1. Wählen Sie in der **Webkonsole** eines bestehenden Clustermitglieds die Registerkarte **System > Clustering > Status** aus, und geben Sie das IVE an, das dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie unter „Angeben eines IVE zum Hinzufügen zu einem Cluster“ auf Seite 236.
2. Verfahren Sie folgendermaßen in der **Webkonsole** des IVE, das einem Cluster hinzugefügt werden soll:

1 Wählen Sie die Registerkarte **System > Configuration > Licensing** aus, und geben Sie den Lizenzcode ein, um die Clusterfunktion zu aktivieren.

2 Wählen Sie die Registerkarte **System > Clustering > Join** aus, und geben Sie Folgendes ein:

- Die Bezeichnung des Clusters, dem das IVE beitreten soll
- Das Clusterkennwort, das Sie beim Definieren des Clusters angegeben haben
- Die IP-Adresse eines aktiven Clustermitglieds

3. Klicken Sie auf **Join Cluster**. Klicken Sie auf **Join**, wenn Sie aufgefordert werden, den Beitritt zum Cluster zu bestätigen. Nachdem das IVE dem Cluster beigetreten ist, müssen Sie sich möglicherweise erneut anmelden.
4. (Nur Access Series FIPS) Initialisieren Sie den Knoten mit der Security World des aktiven Clustermitglieds. Befolgen Sie dazu die folgenden Anweisungen.

So initialisieren Sie die Security World eines FIPS-Clustermitglieds über die serielle Konsole:

1. Schließen Sie das Kabel des Smartcardlesers an den Lesegerätport des Kryptographiemoduls an, der sich an der Frontplatte des IVE-Geräts befindet.
2. Legen Sie eine Administratorkarte, die mit der Security World des aktiven Clustermitglieds vorinitialisiert wurde, mit den Kontakten nach oben in den Smartcardleser ein.
3. Stellen Sie den Modusschalter des Kryptographiemoduls auf **O** (Operationsmodus), sofern dieser sich nicht bereits in dieser Position befindet.
4. Stellen Sie eine Verbindung mit der seriellen Konsole des IVE her. Weitere Informationen finden Sie in Anhang A: auf Seite 567.
5. Schalten Sie das IVE aus und dann wieder ein, und überwachen Sie beim Neustart die serielle Konsole. Nach dem Start der Systemsoftware werden Sie in einer Meldung darüber informiert, dass das Gerät als eigenständiges IVE gestartet wird und dass Sie die **TAB-Taste** drücken müssen, um die Clusteroptionen anzuzeigen. Drücken Sie die **TAB-Taste**, wenn Ihnen diese Meldung angezeigt wird.

   Hinweis: Sie müssen die **TAB-Taste** innerhalb von 5 Sekunden drücken. Wenn das Gerät bereits im eigenständigen Modus bootet, warten Sie, bis der Bootvorgang beendet ist, und starten Sie das Gerät dann neu.

6. Geben Sie die Nummer für den Beitritt zu dem bestehenden Cluster ein.

7. Geben Sie die angeforderten Initialisierungsinformationen ein.

Hinweis: Nachdem Sie die Mitglieder eines Access Series FIPS-Clusters mit derselben Security World initialisiert haben, können Sie den Cluster über die **Webkonsole** deaktivieren und wieder aktivieren. Sie müssen nicht mehr die serielle Konsole verwenden, wenn die Clustermitglieder alle Mitglieder derselben Security World sind.

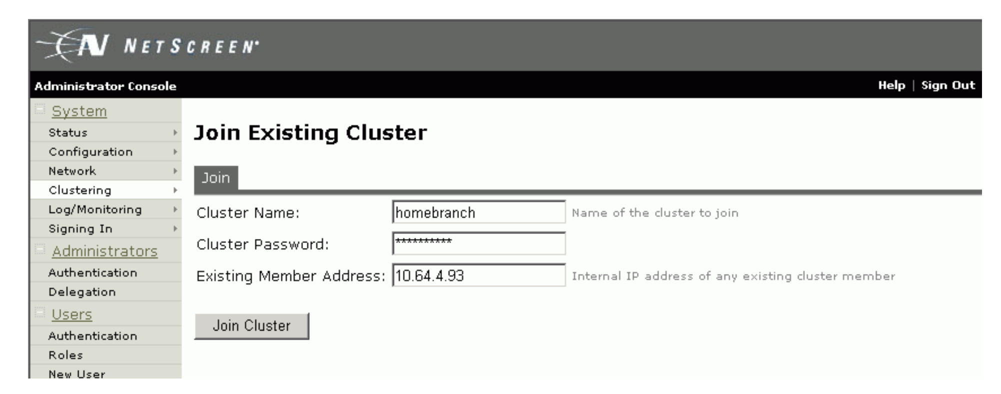


Abbildung 51: System > Clustering > Join – Beitreten zu einem Cluster
Dieses IVE (ive-2) verfügt nicht über dieselbe Lizenz wie das ursprüngliche Clustermitglied ive-1, was anhand der unterschiedlichen Benutzeroberfläche ersichtlich ist.

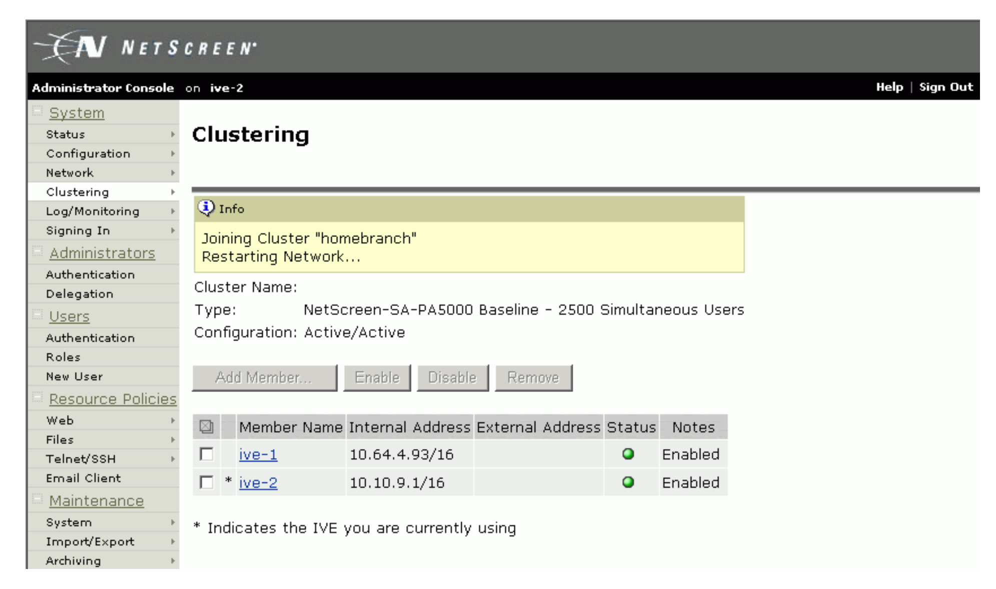


Abbildung 52: System > Clustering > Status – Neustarten von Diensten auf einem neuen Clustermitglied

Während der neue Knoten seinen Status mit dem vorhandenen Clustermitglied synchronisiert, wird der Status der Knoten als „Enabled" oder „Enabled, Transitioning" angezeigt.

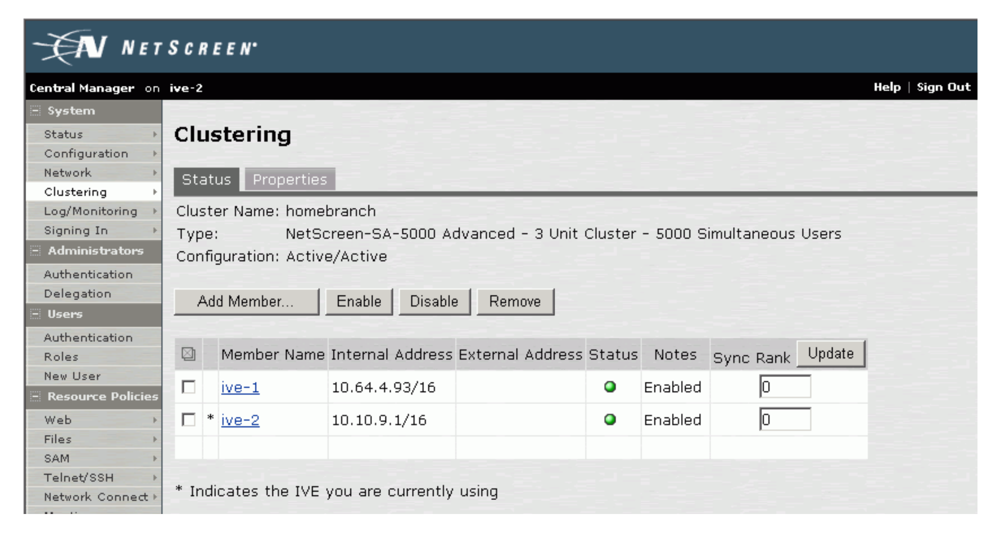


Abbildung 53: System > Clustering > Status – Nach dem Beenden des Knotenübergangs

Nach dem Beitreten des neuen Knotens zum Cluster werden auf seiner Seite **Clustering** die Registerkarten **Status** und **Properties** angezeigt. Die Statusdaten des ursprünglichen Clustermitglieds, darunter System-, Benutzer- und Lizenzdaten, sind auch auf dem neuen Clustermitglied vorhanden. In diesem Beispiel wird die Farbe der Benutzeroberfläche des ursprünglichen Mitglieds im neuen Modus widergespiegelt.

Registerkarte „Status“

Über die Registerkarte **Status** können Sie Folgendes durchführen:

Tabelle 1 auf Seite 240 beschreibt die auf der Registerkarte **Status** angezeigten Informationen und die verschiedenen durchführbaren Verwaltungsaufgaben, darunter das Aktivieren und Deaktivieren eines IVE-Knotens und das Hinzufügen zu bzw. Entfernen dieses Knotens aus einem Cluster.

☑ Angeben eines IVE zum Hinzufügen zu einem Cluster

Bevor ein IVE einem Cluster beitreten kann, müssen Sie seine Netzwerkidentität auf einem aktiven Clustermitglied festlegen.

So geben Sie ein IVE an, das einem bestehenden Cluster hinzugefügt werden soll:

1. Wählen Sie in der **Webkonsole** eines aktiven Clustermitglieds die Registerkarte **System > Clustering > Status** aus.
2. Klicken Sie auf **Add Member**, um ein IVE anzugeben, dass dem Cluster beitritt:
   1. Geben Sie eine Bezeichnung für das Mitglied ein.
   2. Geben Sie die interne IP-Adresse des Geräts ein.
   3. Geben Sie ggf. die externe IP-Adresse des Geräts ein. Beachten Sie, dass das Adressfeld **External IP** nur angezeigt wird, wenn Sie den externen Port auf der Registerkarte **System > Network > External Port** aktiviert haben.
   4. Ändern Sie ggf. die Netzmasken- und Gatewayeinstellungen für den Knoten.
   5. Klicken Sie auf **Add Node**.
   6. Klicken Sie auf **Add**, wenn Sie aufgefordert werden, das Hinzufügen des neuen Mitglieds zu bestätigen.

7 Wiederholen Sie diesen Vorgang für alle IVEs, die Sie zu einem Cluster hinzufügen möchten.

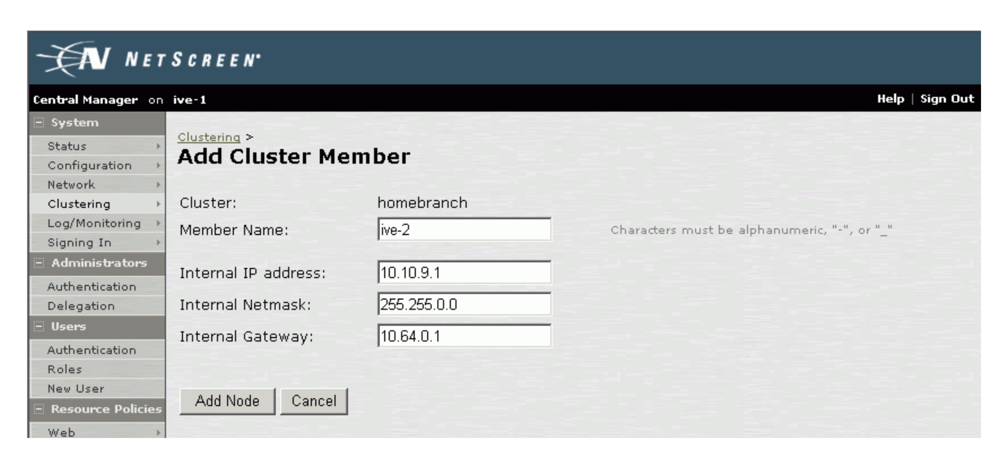


Abbildung 54: System > Clustering > Status – Festlegen eines IVE zum Hinzufügen zu einem Cluster

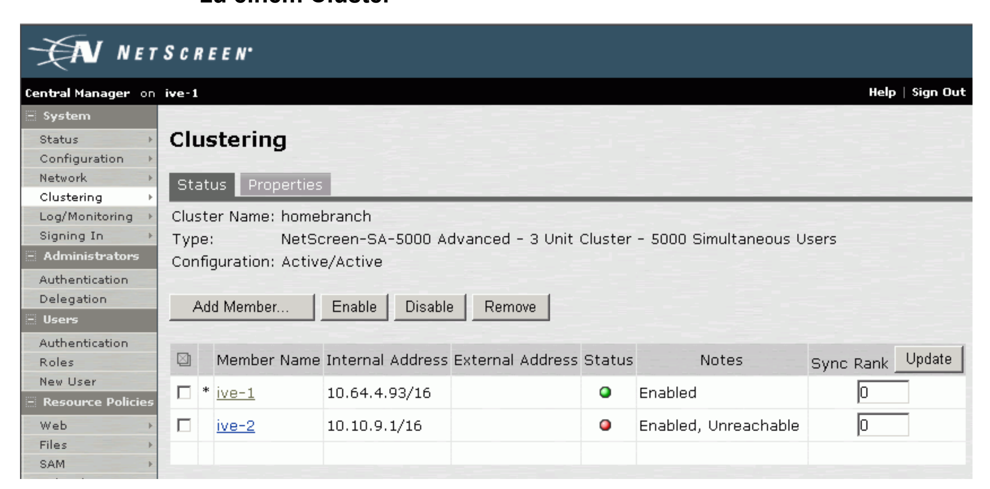


Abbildung 55: System > Clustering > Status – Nach dem Festlegen eines neuen Mitglieds

☑ Verwalten von Netzwerkeinstellungen für Clusterknoten

Änderungen an den Netzwerkeinstellungen für einen Cluster oder an den einzelnen Knoten darin können Sie über die Seiten **System > Network** durchführen. Nach dem Erstellen eines Clusters wird auf diesen Seiten eine Dropdownliste angezeigt, in der Sie einen ganzen Cluster oder einen bestimmten Knoten zum Ändern auswählen können. Beim Speichern von Änderungen auf der Seite **Network** werden die Einstellungen für den angegebenen Cluster oder Clusterknoten gespeichert. Wenn Sie Netzwerkeinstellungen für einen gesamten Cluster ändern, werden sie auf jeden Knoten im Cluster übertragen.

Hinweis: Sie können auf eine knotenspezifische Seite **Network** zugreifen, indem Sie in der Spalte **Member Name** der Registerkarte **Clustering > Status** auf den Namen des Knotens klicken.

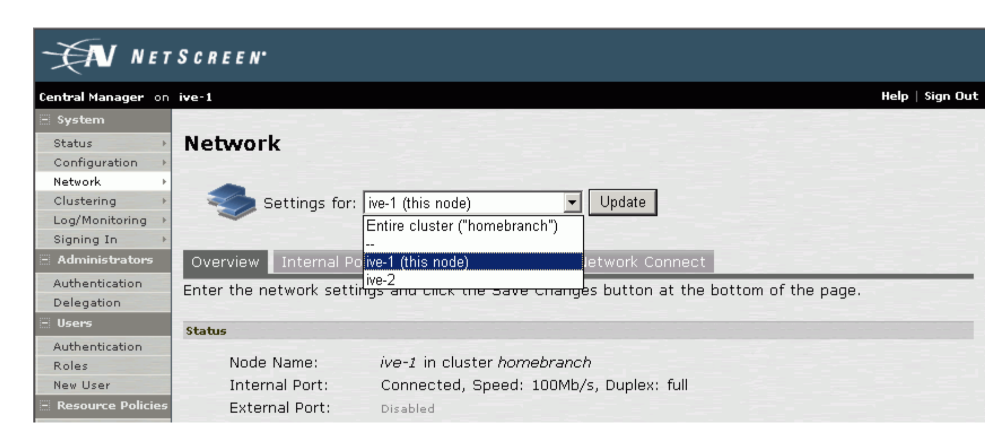


Abbildung 56: **Seiten „System > Network“**

☑ Deaktivieren von Knoten zum Aktualisieren des Clusterdienstpakets

Wenn Sie Juniper Networks NetScreen-SA Central Manager erworben haben, müssen Sie einfach nur ein neueres Dienstpaket auf einem Clusterknoten installieren. Wenn der Installationsprozess abgeschlossen ist und der Clusterknoten neu startet, weist er die anderen Knoten zur Aktualisierung an. Weitere Informationen zum Installieren eines Dienstpakets finden Sie unter „Installieren eines Juniper Networks-Softwaredienstpakets“ auf Seite 526.

Wenn Sie Juniper Networks NetScreen-SA Central Manager nicht ausführen, müssen Sie einen Knoten manuell deaktivieren, sein Dienstpaket aktualisieren und nach Abschluss der Aktualisierung den Knoten aktivieren.

Wichtig: Sie können Clustermitglieder nicht auf Dienstpaketversionen herunterstufen, die älter als das momentan installierte Paket sind. Sie können die einzelnen Clustermitglieder aber auf ihren vorherigen Nicht-Cluster-Zustand zurückstufen, indem Sie zuerst alle Knoten des Clusters deaktivieren und dann die in Anhang A: auf Seite 567 beschriebene Rollbackfunktion ausführen.

So deaktivieren Sie Knoten zum Aktualisieren eines Clusterdienstpakets:

1. Melden Sie sich bei der **Webkonsole** des Knotens an, den Sie aktualisieren möchten.
2. Wählen Sie **Clustering > Status** aus, aktivieren Sie das Kontrollkästchen neben dem Knotennamen, und klicken Sie dann auf **Disable**.
3. Folgen Sie den Anweisungen zum Installieren des Dienstpakets unter „Installieren eines Juniper Networks-Softwaredienstpakets“ auf Seite 526.
4. Wechseln Sie zu **Clustering > Status** zurück, aktivieren Sie das Kontrollkästchen neben dem Knotennamen, und klicken Sie dann auf **Enable**.

Tabelle 1: Clustering > Registerkarte „Status“

Element der Benutzeroberfläche	Beschreibung
Schaltfläche **Add Member**	Klicken Sie auf diese Schaltfläche, um ein IVE anzugeben, das dem Cluster beitreten soll. Diesen Schritt müssen Sie für jedes IVE durchführen, das Sie dem Cluster hinzufügen möchten.
Schaltfläche **Enable**	Klicken Sie auf diese Schaltfläche, um einen zuvor deaktivierten Knoten zu aktivieren. Wenn Sie einen Knoten wieder aktivieren, werden alle Statusinformationen auf dem Knoten synchronisiert.
Schaltfläche **Disable**	Klicken Sie auf diese Schaltfläche, um einen Knoten in einem Cluster zu deaktivieren. Der Knoten kommuniziert noch mit dem Cluster, ist jedoch für Statussynchronisierungen deaktiviert und empfängt keine Benutzeranforderungen mehr, es sei denn, der Benutzer meldet sich direkt bei diesem Knoten an.
Schaltfläche **Remove**	Klicken Sie auf diese Schaltfläche, um den oder die ausgewählten Knoten aus dem Cluster zu entfernen. Nachdem der Knoten entfernt wurde, wird er im eigenständigen Modus ausgeführt.
Spalte **Member Name**	Führt alle Knoten auf, die zu dem Cluster gehören. Sie können auf einen Knotennamen klicken, um seinen Namen und die Netzwerkeinstellungen zu ändern.
Spalte **Internal IP Address**	Gibt die interne IP-Adresse des Clustermitglieds in der CIDR-Schreibweise (Classless Inter Domain Routing) an.
Spalte **External IP Address**	Gibt die externe IP-Adresse des Clustermitglieds in der CIDR-Schreibweise (Classless Inter Domain Routing) an. Beachten Sie, dass diese Spalte nur die externe IP-Adresse des Clusterleiters enthält, es sei denn, Sie geben auf seiner eigenen Seite für Netzwerkeinstellungen eine andere Adresse für den Knoten an. Zum Öffnen dieser Seite klicken Sie in der Spalte **Member Name** auf den Namen des Knotens. Wenn Sie die externe IP-Adresse auf der Seite **Network > Network Settings** ändern, wirkt sich die Änderung auf alle Clusterknoten aus.

Tabelle 1: Clustering > Registerkarte „Status“ fortgesetzt

Element der Benutzeroberfläche	Beschreibung
Spalte **Status**	Gibt den Status des Knotens an: • **Grünes Licht/Enabled** – Der Knoten bearbeitet Benutzeranforderungen und nimmt an der Clustersynchronisierung teil. • **Gelbes Licht/Transitioning** – Der Knoten tritt dem Cluster bei. • **Rotes Licht/Disabled** – Der Knoten bearbeitet keine Benutzeranforderungen und nimmt nicht an der Clustersynchronisierung teil. **Hinweis:** Der Status eines Knotens wird als „eigenständig“ betrachtet, wenn der Knoten außerhalb eines Clusters bereitgestellt wird oder aus einem Cluster entfernt wurde.
Spalte **Notes**	Gibt den Status der Verbindung des Knotens mit dem Cluster an. Der Status kann folgendermaßen lauten: • OK – Der Knoten ist aktiver Bestandteil des Clusters. • Transitioning – Der Knoten wechselt vom eigenständigen Status in den aktivierten Status. • Unreachable – Der Knoten kommuniziert nicht mehr mit dem Cluster. Ein Clustermitglied kann selbst dann „unreachable“ sein, wenn es online ist und über einen Ping-Befehl erreicht wird. Mögliche Gründe sind: Sein Kennwort ist falsch, es kommuniziert nicht mit allen Clusterknoten, es ist mit einem anderen Gruppen-kommunikationsmodus konfiguriert, es führt eine andere Version des Dienstpakets aus oder das IVE ist ausgeschaltet.
Spalte **Sync Rank**	Legt die Reihenfolge fest, in der die Clusterknoten synchronisiert werden sollen. **Hinweis:** Diese Option steht nur mit einer Central Manager-Lizenz zur Verfügung.

Registerkarte „Properties“

Auf der Registerkarte **Properties** können Sie Folgendes durchführen:

☑ Festlegen von Aktiv/Passiv, Aktiv/Aktiv und anderen Cluster-einstellungen:

Auf der Registerkarte **Properties** können Sie den Namen eines Clusters ändern, die Ausführungskonfiguration eines Clusters (Aktiv/Passiv oder Aktiv/Aktiv) angeben, Überprüfungseinstellungen („Healthcheck“) für Synchronisierung und Netzwerk festlegen und einen Cluster löschen.

So ändern Sie Clustereigenschaften

1. Wählen Sie in der **Webkonsole** eines aktiven Clustermitglieds die Registerkarte **System > Clustering > Status** aus.
2. Bearbeiten Sie das Feld **Cluster Name**, um den Namen des Clusters zu ändern (optional).
3. Wählen Sie unter **Configuration Settings** Folgendes aus:
   - **Active/Passive** zum Ausführen eines Clusterpaares im Aktiv/Passiv-Modus. Geben Sie dann eine interne VIP (virtuelle IP-Adresse) und, sofern der externe Port aktiviert ist, eine externe VIP an.

     Hinweis: Um einen Cluster mit zwei Einheiten im Aktiv/Passiv-Modus auszuführen, müssen sich die IVEs im gleichen Subnetzwerk befinden.

   - **Active/Active** zum Ausführen eines Clusters mit zwei oder mehr Knoten im Aktiv/Aktiv-Modus unter Verwendung eines externen Load-Balancers.

     Hinweis: Wenn Sie einen Aktiv/Passiv-Cluster mit zwei Einheiten in einen Aktiv/Aktiv-Cluster mit mehr als zwei Knoten ändern möchten, ändern Sie zuerst die Konfiguration des Clusters mit zwei Einheiten auf Aktiv/Aktiv und fügen dann die zusätzlichen Knoten hinzu.

4. Wählen Sie unter **Synchronization Settings** Folgendes aus:
   - Ein Synchronisierungsprotokoll zur Verwendung beim Synchronisieren von Daten zwischen Knoten (eine Beschreibung der Synchronisierungseinstellungen finden Sie unter „Statussynchronisierung" auf Seite 83)
   - Den Typ der zu synchronisierenden Daten, einschließlich Protokollmeldungen und Benutzerdaten
5. Geben Sie unter **Network Healthcheck Settings** die zulässige Höchstanzahl von ARP-Pingfehlern an, die stattfinden dürfen, bevor die interne Schnittstelle des IVE deaktiviert wird, und legen Sie fest, ob die externe Schnittstelle des IVE deaktiviert werden soll, wenn die interne Schnittstelle ausfällt.

☑ Löschen eines Clusters

Wenn Sie einen Cluster löschen, werden alle Knoten als eigenständige IVEs ausgeführt.

So löschen Sie einen Cluster:

1. Wählen Sie in der **Webkonsole** eines aktiven Clustermitglieds die Registerkarte **System > Clustering > Properties** aus.
2. Wählen Sie **Delete Cluster** aus. Nach Beendigung des Vorgangs werden alle Clusterknoten als eigenständige IVEs ausgeführt.

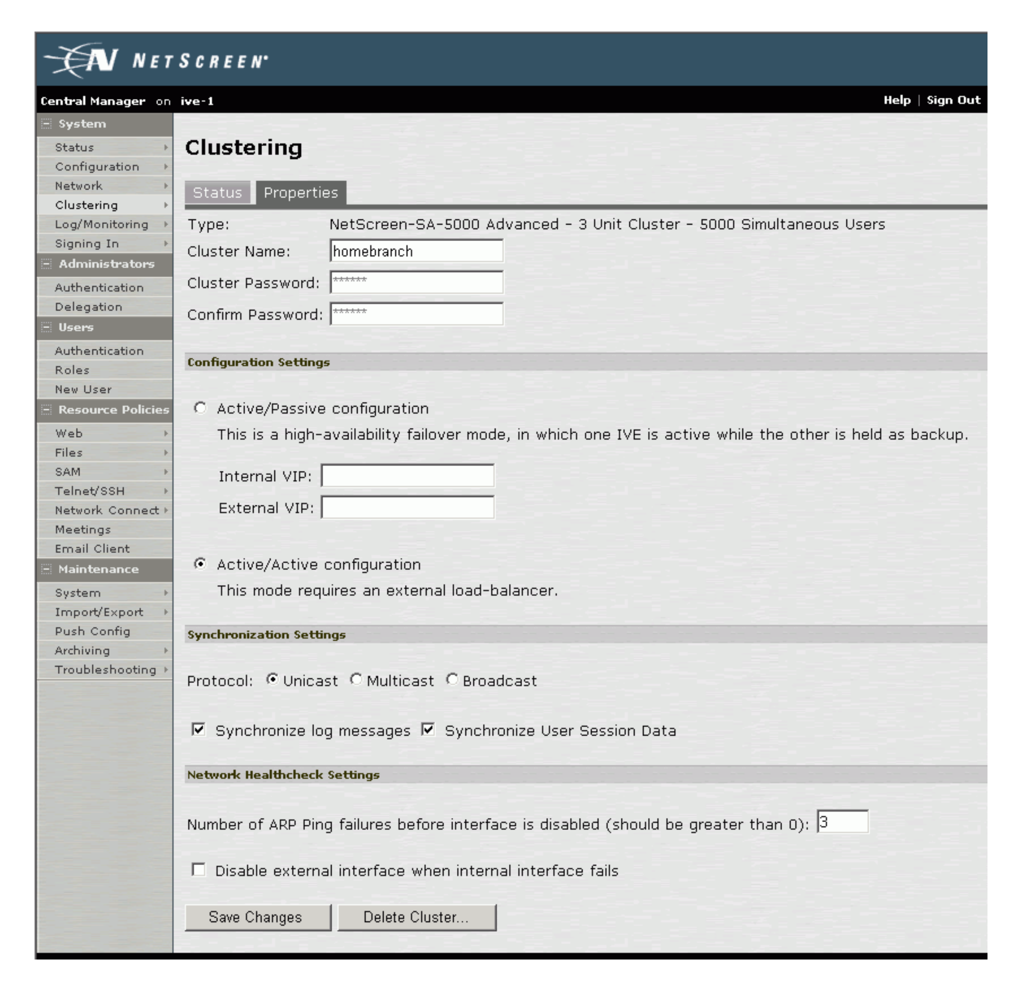


Abbildung 57: System > Clustering > Properties

Verfahren über die serielle Konsole

Sie können ein IVE über seine serielle Konsole zu einem Cluster hinzufügen, es sei denn, diese wird in einer Access Series FIPS-Umgebung ausgeführt. In letzterem Fall müssen Sie jedes IVE über seine Webkonsole hinzufügen. Wenn Sie ein werkseitig eingestelltes IVE zu einem Cluster hinzufügen, empfiehlt es sich, die serielle Konsole zu verwenden. Der Beitritt zu einem bestehenden Cluster kann dann im Verlauf des Initialisierungsvorgangs unter Eingabe nur weniger Informationen erfolgen. Wenn ein IVE einem Cluster beitritt, empfängt es die Clusterstatuseinstellungen. Dabei werden *alle* Einstellungen auf einem IVE mit einer bestehenden Konfiguration überschrieben, und neuen Geräten werden die erforderlichen Vorabinformationen bereitgestellt.

☑ Hinzufügen eines IVE zu einem Cluster über die serielle Konsole

Ein werkseitig eingestelltes oder konfiguriertes IVE kann einem Cluster erst hinzugefügt werden, wenn dem Cluster dessen Identität bekannt ist. Anweisungen zur Angabe eines IVE, dass einem Cluster hinzugefügt werden soll, finden Sie unter „Angeben eines IVE zum Hinzufügen zu einem Cluster“ auf Seite 236.

Wichtig: Wenn Sie ein IVE, das gegenwärtig als eigenständiges Gerät ausgeführt wird, über seine **Webkonsole** zu einem Cluster hinzufügen möchten, muss dasselbe oder ein älteres Dienstpaket auf der gleichen Hardwareplattform wie bei den anderen Mitgliedern ausgeführt werden.

So fügen Sie ein IVE über seine serielle Konsole zu einem Cluster hinzu:

1. Wählen Sie in der **Webkonsole** eines bestehenden Clustermitglieds die Registerkarte **System > Clustering > Status** aus, und geben Sie das IVE an, das dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie unter „Angeben eines IVE zum Hinzufügen zu einem Cluster“ auf Seite 236.
2. Stellen Sie eine Verbindung mit der seriellen Konsole des IVE her, dass dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie in Anhang A: auf Seite 567.

3. Schalten Sie das IVE aus und dann wieder ein, und überwachen Sie beim Neustart die serielle Konsole. Nach dem Start der Systemsoftware werden Sie in einer Meldung informiert, dass das Gerät als eigenständiges IVE gestartet wird und dass Sie die **TAB-Taste** drücken müssen, um die Clusteroptionen anzuzeigen. Drücken Sie die **TAB-Taste**, wenn Ihnen diese Meldung angezeigt wird.

Hinweis: Sie müssen die **TAB-Taste** innerhalb von 5 Sekunden drücken. Wenn das Gerät bereits im eigenständigen Modus bootet, warten Sie, bis der Bootvorgang beendet ist, und starten Sie das Gerät dann neu.

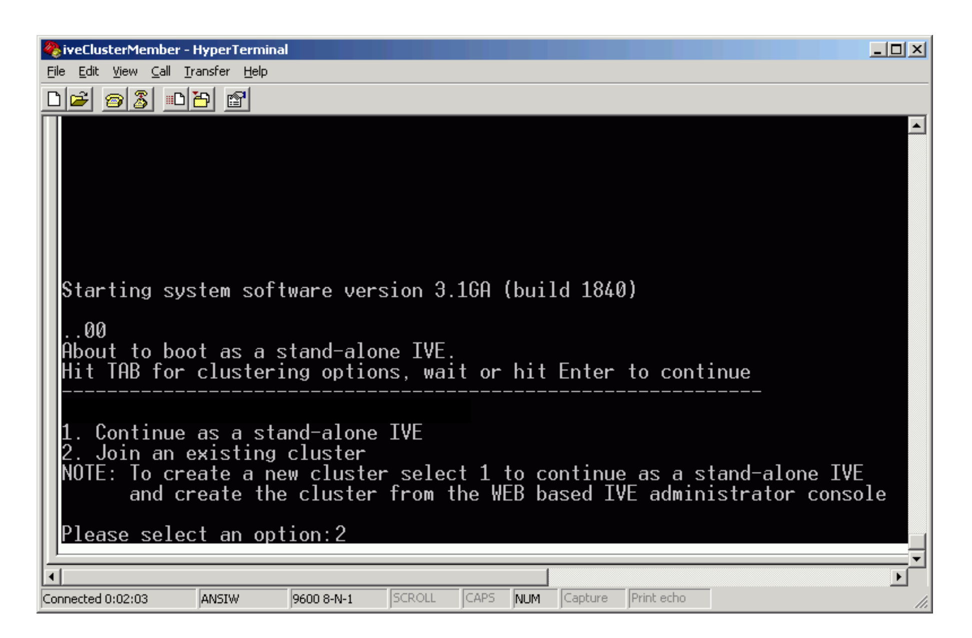


Abbildung 58: **Serielle Konsole – Option für Clusterbeitritt**

4. Geben Sie die Nummer für den Beitritt zu einem bestehenden Cluster ein.

5. Geben Sie die erforderlichen Informationen ein. Dies sind:

- Die interne IP-Adresse eines aktiven Clustermitglieds.
- Das Clusterkennwort, d. h. das Kennwort, dass Sie beim Definieren des Clusters eingegeben haben.
- Der Name des Geräts, das Sie hinzufügen möchten. In diesem Beispiel lautet der Name `ive-2`.
- Die interne IP-Adresse des Geräts, das Sie hinzufügen möchten.
- Die Netzmaske des Geräts, das Sie hinzufügen möchten.
- Das Gateway des Geräts, das Sie hinzufügen möchten.

Das aktive Clustermitglied überprüft das Clusterkennwort und stellt sicher, dass der Name und die IP-Adresse des neuen Computers mit Ihren Angaben in der Webkonsole auf der Seite **System > Clustering > Add Cluster Member** übereinstimmen. Wenn die Anmeldeinformationen gültig sind, überträgt das aktive Mitglied sämtliche Statusdaten auf das neue Clustermitglied, einschließlich Lizenz-, Zertifikats-, Benutzer- und Systemdaten.

iveClusterMember - HyperTerminal

File Edit View Call Transfer Help

```
..00
About to boot as a stand-alone IVE.
Hit TAB for clustering options, wait or hit Enter to continue
--------------------------------------------------------------
0. Start a shell (debug builds only)
1. Continue as a stand-alone IVE
2. Join an existing cluster
NOTE: To create a new cluster select 1 to continue as a stand-alone IVE
      and create the cluster from the WEB based IVE administrator console

Please select an option: 2

Please provide the following information:
Internal IP address of an active cluster member []:10.10.9.1
Cluster password:
Name of this host in the cluster []:            ive-2
Internal IP address for this host []:           10.12.173.2
Netmask for this host []:                       255.255.0.0
Gateway for this host []:                       10.10.0.1
Contacting host with internal IP '10.10.9.1'
...
```

Connected 0:24:29 | ANSIW | 9600 8-N-1 | SCROLL | CAPS | NUM | Capture | Print echo

Abbildung 59: **Serielle Konsole – Angeben des neuen Clustermitglieds**

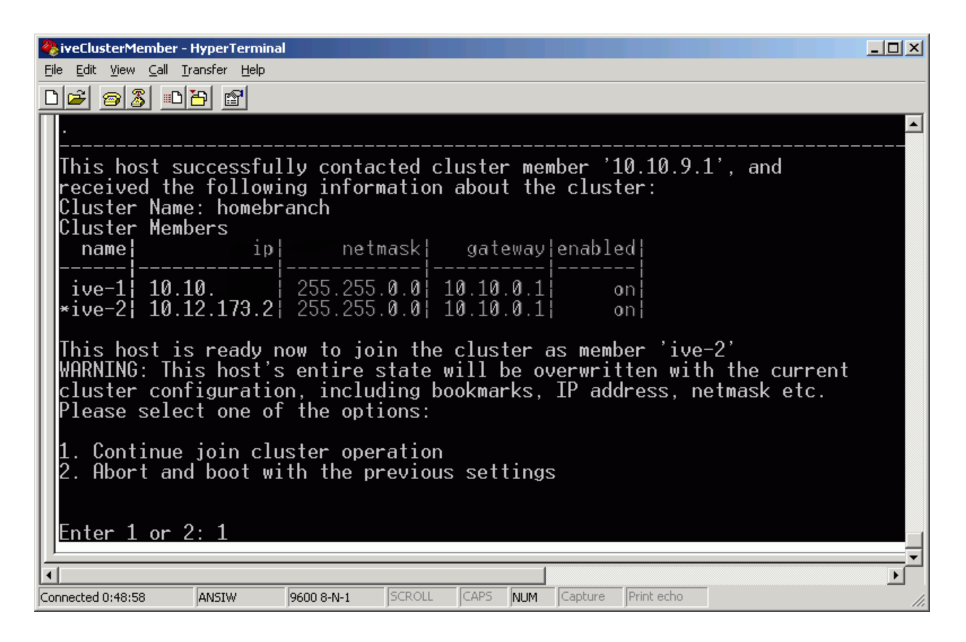


Abbildung 60: Serielle Konsole – Bestätigen des Clusterbeitritts

6. Geben Sie zum Fortfahren die Nummer ein. Wenn die Bestätigungsmeldung für den Beitritt des Geräts zum Cluster angezeigt wird, überprüfen Sie auf der Registerkarte **System > Clustering > Status** von allen aktiven Clustermitgliedern, ob der **Status** des neuen Mitglieds als grünes Licht angezeigt wird, d. h., dass das IVE ein aktiver Knoten des Clusters ist.

Konfigurieren der Seite „Log Monitoring“

Die Seite **System > Log Monitoring** enthält die folgenden Registerkarten:

Auf der Seite **System > Log Monitoring** können Sie Folgendes durchführen:

Weitere Informationen zu Protokollen und Überwachungsfunktionen des IVE finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 103.

Registerkarten „Events“, „User Access“ und „Admin Access“

Auf den Seiten **System > Log/Monitoring > Events**, **User Access** und **Admin Access** können Sie das Ereignisprotokoll (das die Systemereignisse enthält), das Benutzerzugriffsprotokoll (das die Endbenutzeranforderungen und -änderungen enthält) und das Administratorzugriffsprotokoll (das die Administratoränderungen enthält) filtern und formatieren.

Die Seiten **Events**, **User Access** und **Admin Access** enthalten jeweils die folgenden Registerkarten:

Hinweis: Bei den Ereignis-, Benutzerzugriffs- und Administratorzugriffsprotokollen handelt es sich um drei eigenständige Dateien. Obwohl die grundlegenden Konfigurationsanweisungen für alle drei gleich sind, wirken sich Einstellungsänderungen bei einer der Dateien nicht auf die Einstellungen der anderen aus. Weitere Informationen zu den Inhalten der einzelnen Dateien finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 103.

Registerkarte „Log“

☑ Speichern, Anzeigen oder Löschen der Protokolldatei

So zeigen Sie die Ereignisprotokolldatei an, speichern sie oder löschen sie:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.
2. Klicken Sie auf die Registerkarte **Events**, **User Access** oder **Admin Access**, und wählen Sie dann **Log** aus.
3. (Gilt nur für Central Manager) Wählen Sie aus der Liste **View by filter** den benutzerdefinierten Filter aus, den das IVE zum Filtern von Daten verwenden sollte.
4. Geben Sie im Feld **Show** eine Nummer ein, und klicken Sie auf **Update**, wenn Sie die Anzahl der jeweils vom IVE angezeigten Protokolleinträge ändern möchten.
5. Klicken Sie auf **Save Log As**, wechseln Sie zum gewünschten Netzwerkspeicherort, geben Sie einen Dateinamen ein, und klicken Sie dann auf **Save**, um die Protokolldatei manuell zu speichern.
6. Klicken Sie auf **Clear Log**, um das lokale Protokoll und die Datei `log.old` zu löschen.

Hinweis: Wenn Sie das lokale Protokoll löschen, wirkt sich dies nicht auf die vom Syslog-Server aufgezeichneten Ereignisse aus. Die nachfolgenden Ereignisse werden in einer neuen lokalen Protokolldatei aufgezeichnet.

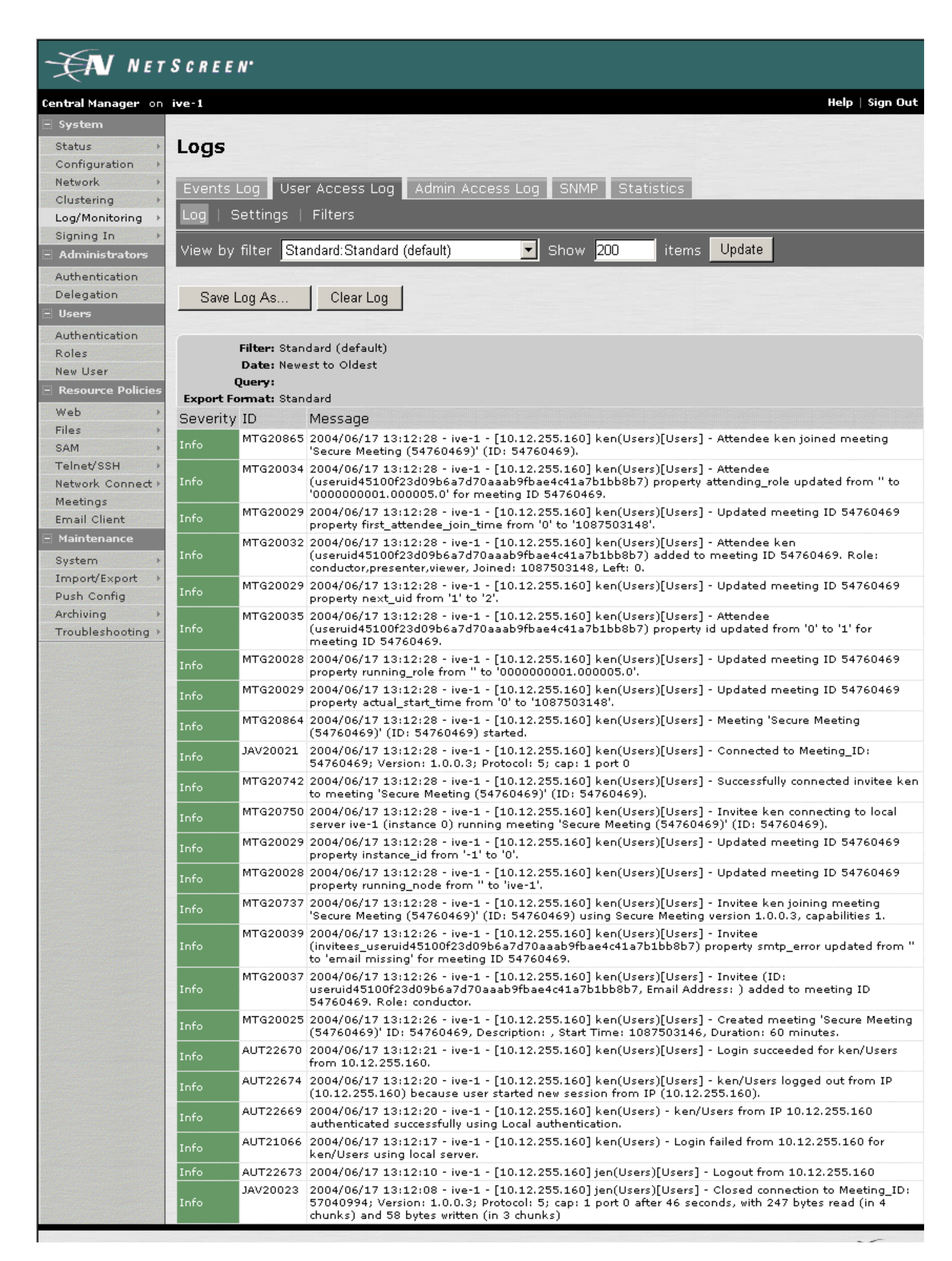


Abbildung 61: System > Log/Monitoring > User Access Log > Log

Registerkarte „Einstellungen“

☑ Geben Sie an, welche Ereignisse in der Protokolldatei gespeichert werden sollen

Mithilfe der Optionen auf der Registerkarte **Settings** können Sie neben der Höchstdateigröße angeben, was das IVE in die Protokolldatei schreiben und welcher Syslog-Server zum Speichern der Protokolldateien verwendet werden soll.

Hinweis: Sie können auch die Seite **Archiving** verwenden, um die Protokolle automatisch an einem für FTP zugänglichen Ort zu speichern. Weitere Informationen finden Sie unter „Konfigurieren der Seite „Archiving““ auf Seite 541.

So legen Sie die Einstellungen für das Ereignisprotokoll fest:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.
2. Klicken Sie auf die Registerkarte **Events**, **User Access** oder **Admin Access**, und wählen Sie dann **Settings** aus.
3. Geben Sie in der Liste **Max Log Size** die Höchstdateigröße für die lokale Protokolldatei an. (Die Grenze liegt bei 500 MB.) Im Systemprotokoll werden Daten bis zu der angegebenen Menge angezeigt.

   Hinweis: Max Log Size ist eine interne Einstellung, die weitgehend der Größe von Protokollen entspricht, die mit **Standard** formatiert werden. Wenn Sie ein ausführlicheres Format, wie z. B. **WELF** auswählen, kann die Protokolldatei die hier angegebene Größe überschreiten.

   ---

4. Aktivieren Sie unter **Select Events to Log** die Kontrollkästchen für die einzelnen Ereignisarten, die in der lokalen Protokolldatei erfasst werden sollen.

   Hinweis: Wenn Sie das Kontrollkästchen **Statistics** auf der Registerkarte **Events** deaktivieren, schreibt das IVE die Statistiken nicht in die Protokolldatei, sondern zeigt sie weiterhin auf der Registerkarte **System > Log/Monitoring > Statistics** an (Seite 264).

   ---

5. Geben Sie unter **Syslog Servers** Informationen über den Syslog-Server ein, auf dem die Protokolldateien gespeichert werden sollen (optional):
   1. Geben Sie den Namen oder die IP-Adresse des Syslog-Servers ein.
   2. Geben Sie einen Syslog-Typ („Facility“) für den Server ein. Das IVE stellt 8 Facilitys (LOCAL0-LOCAL7) bereit, die Sie den Facilitys auf dem Syslog-Server zuordnen können.

3. (Gilt nur für Central Manager) Wählen Sie den Filter, den Sie auf die Protokolldatei anwenden möchten.
4. Klicken Sie auf **Add**.
5. Wiederholen Sie den Vorgang ggf. für mehrere Server, und verwenden Sie unterschiedliche Formate und Filter für verschiedene Server und Facilitys.

Wichtig: Vergewissern Sie sich, dass der Syslog-Server Nachrichten mit den folgenden Einstellungen akzeptiert: `facility = LOG_USER` und `level = LOG_INFO`.

---

6. Klicken Sie auf **Save Changes**.

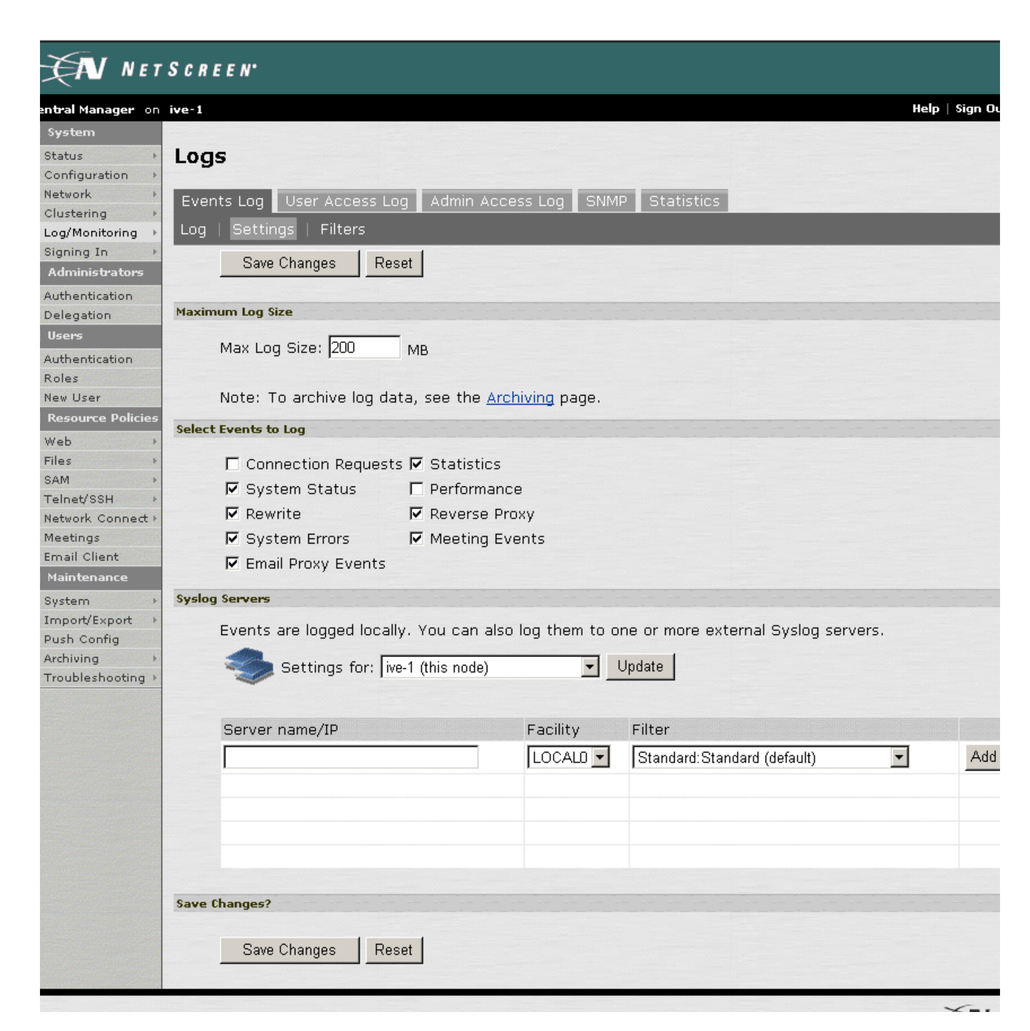


Abbildung 62: System > Log/Monitoring > Events Log > Settings

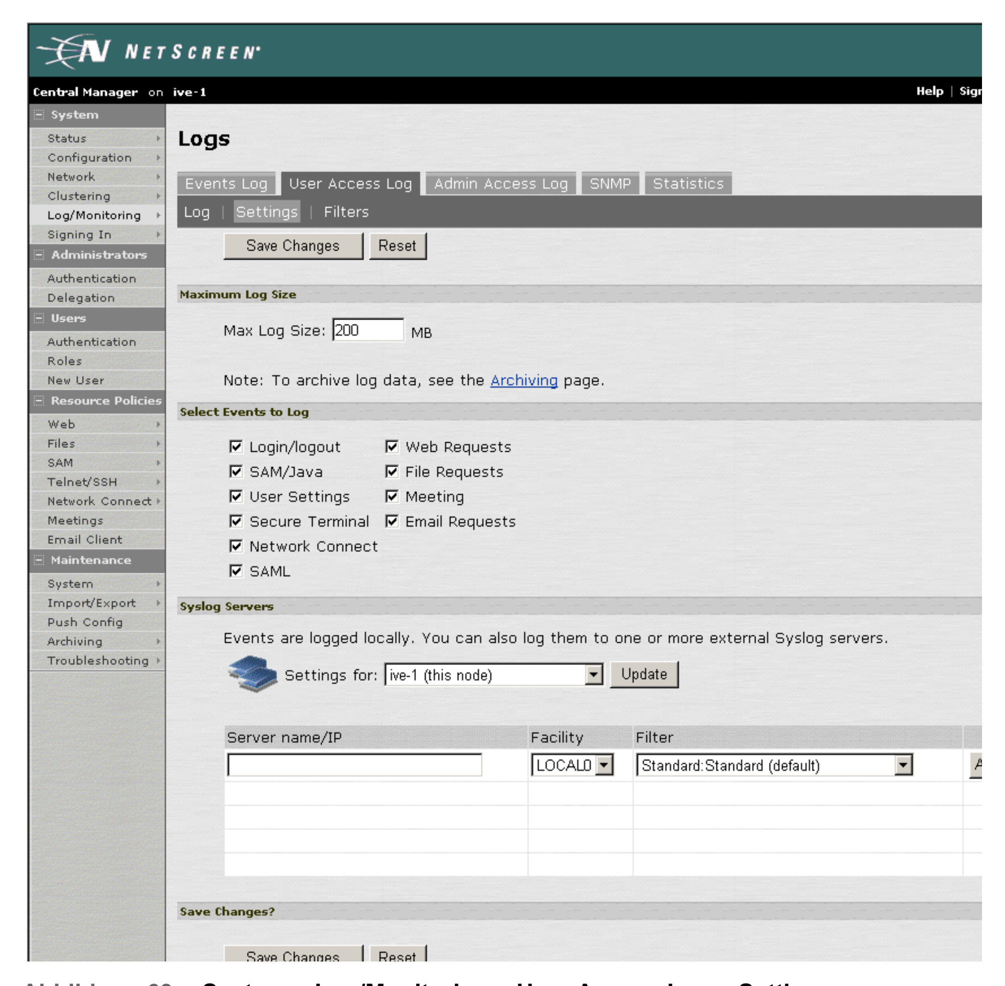


Abbildung 63: System > Log/Monitoring > User Access Log > Settings

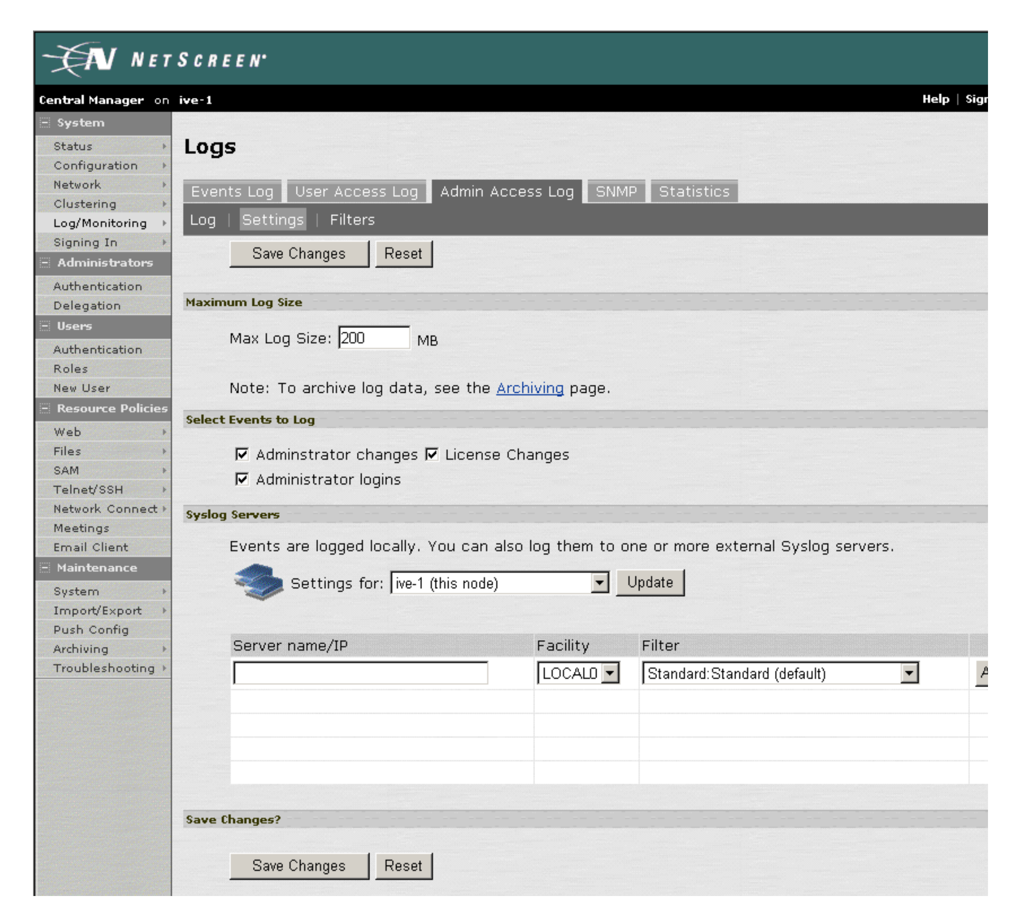


Abbildung 64: **System > Log/Monitoring > Admin Access Log > Settings**

Registerkarte „Filters“

☑ Erstellen von benutzerdefinierten Filtern und Formaten für Protokolldateien

Mithilfe der Optionen auf der Registerkarte **Filters** können Sie angeben, welche Daten in den Protokolldateien erfasst werden und welches Format verwendet wird. Diese Option ist nur mit dem Central Manager-Paket verfügbar.

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.
2. Klicken Sie auf die Registerkarte **Events**, **User Access** oder **Admin Access**, und wählen Sie dann **Filters** aus.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Um einen bestehenden Filter zu ändern, klicken Sie auf seinen Namen.
   - Um einen neuen Filter zu erstellen, klicken Sie auf **New Filter**.
4. Geben Sie eine Bezeichnung für den Filter ein.

Wichtig: Wenn Sie ein Format auswählen und dann im Feld **Filter Name** eine neue Bezeichnung angeben, erstellt das IVE kein neues benutzerdefiniertes Filterformat, das auf dem bestehenden Format basiert. Stattdessen überschreibt es das bestehende Format mit den von Ihnen vorgenommenen Änderungen.

---

5. Klicken Sie auf **Make Default**, um den ausgewählten Filter als Standard-Protokolldateityp festzulegen. Sie können für die Ereignis-, Benutzerzugriffs- und Administratorzugriffsprotokolle jeweils unterschiedliche Standardfilter einstellen.
6. Anhand der Optionen im Abschnitt **Query** können Sie die Auswahl der Daten steuern, die das IVE ins Protokoll schreibt:
   1. Klicken Sie im Abschnitt **Start Date** auf **Earliest Date**, damit alle Protokolle ab dem ersten verfügbaren Datum geschrieben werden, das in der Protokolldatei gespeichert ist. Sie können auch manuell ein Startdatum eingeben.
   2. Klicken Sie im Abschnitt **End Date** auf **Latest Date**, damit alle Protokolle bis zum letzten verfügbaren Datum geschrieben werden, das in der Protokolldatei gespeichert ist. Sie können auch manuell ein Enddatum eingeben.
   3. Verwenden Sie die Sprache für benutzerdefinierte Ausdrücke des IVE im Abschnitt **Query**, um die Auswahl der Daten zu steuern, die das IVE ins Protokoll schreibt.

7. Sie können eine der Optionen aus dem Abschnitt **Export Format** verwenden, um das Datenformat im Protokoll zu steuern:
   - Wählen Sie die Option **Standard**, **WELF** oder **W3C** aus, um die Protokolleinträge mithilfe eines dieser standardisierten Formate zu formatieren. Weitere Informationen finden Sie unter „Benutzerdefinierte Filterung von Protokolldateien" auf Seite 105.
   - Wählen Sie die Option **Custom** aus, und geben Sie das Format ein, das im Feld **Format** verwendet werden soll. Schließen Sie Variablen bei der Eingabe des Formats in Prozentzeichen ein (z. B. %user%). Alle anderen Zeichen im Feld werden als Literalzeichen behandelt.
8. Klicken Sie auf **Speichern**.

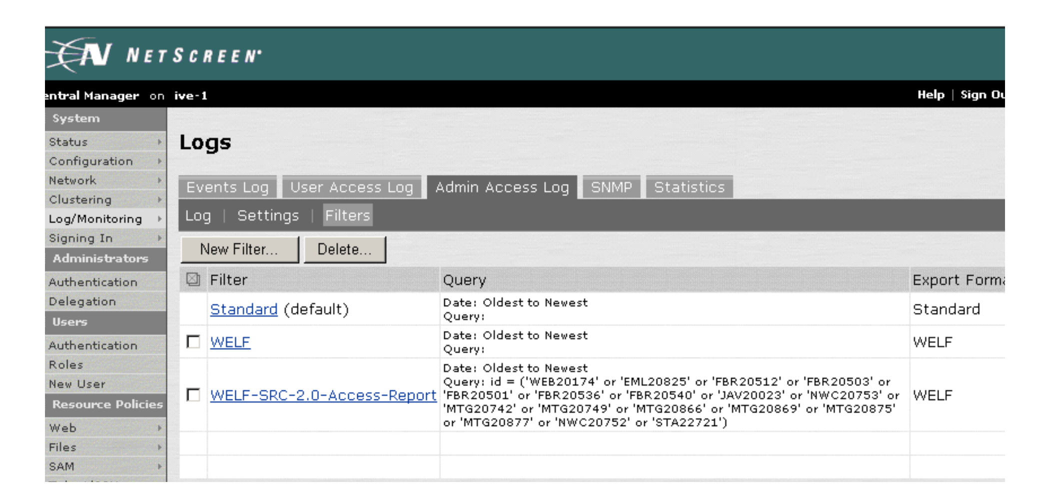


Abbildung 65: System > Log/Monitoring > Admin Access Logs > Filters

Registerkarte „SNMP“

☑ Überwachen des IVE als SNMP-Agent

Über diese Registerkarte können Sie ein Netzwerkverwaltungstool wie HP OpenView zum Überwachen des IVE als SNMP-Agent verwenden. Das IVE unterstützt SNMP (Simple Network Management Protocol), Version 2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die NetScreen-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen.

Hinweis: Zum Überwachen wesentlicher IVE-Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse: http://net-snmp.sourceforge.net/UCD-SNMP-MIB.txt.

So legen Sie SNMP-Einstellungen fest:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring > SNMP** aus.
2. Klicken Sie auf die Verknüpfung **NetScreenMIB file**, um auf die MIB-Datei zuzugreifen, und speichern Sie die Datei dann im Browser an einem Netzwerkspeicherort. (Eine Beschreibung der Get- und Trap-Objekte in der MIB-Datei finden Sie in den folgenden Tabellen.)
3. Geben Sie unter **Agent Properties** Informationen in die folgenden Felder ein, und klicken Sie anschließend auf **Save Changes**:
   - Geben Sie in die Felder **System Name**, **System Location** und **System Contact** Informationen ein, die den IVE-Agent beschreiben (optional).
   - Geben Sie im Feld **Community** eine Zeichenfolge ein (erforderlich).

   Hinweis: Zum Abfragen des IVEs muss Ihre Netzwerkverwaltungsstation diese Zeichenfolge an das IVE senden. Um den SNMP-Daemon zu beenden, löschen Sie die Angaben im Feld **Community**.

4. Legen Sie unter **Traps** die Server fest, an die das IVE Traps senden soll, die es bei Eingabe von Daten in die folgenden Felder generiert, und klicken Sie anschließend auf **Add**:
   - Der Hostname oder die IP-Adresse des Servers
   - Der Port, an dem der Server Daten abfragt (üblicherweise Port 162)
   - Die von der Netzwerkverwaltungsstation benötigte Community-Zeichenfolge (sofern vorhanden)
5. Klicken Sie auf **Save Changes**.
6. Gehen Sie in der Netzwerkverwaltungsstation folgendermaßen vor:
   1. Laden Sie die NetScreen-MIB-Datei herunter.
   2. Geben Sie die Community-Zeichenfolge an, die beim Abfragen des IVE benötigt wird (siehe Schritt 3).
   3. Konfigurieren Sie die Netzwerkverwaltungssoftware für den Empfang von IVE-Traps.

Tabelle 1: NetScreen-MIB-Objekte: Gets

Objekt	Beschreibung
logFullPercent	Gibt den Prozentsatz der verfügbaren Dateigröße zurück, der durch das aktuelle Protokoll belegt wird.
signedInWebUsers	Gibt die Anzahl der über einen Webbrowser beim IVE angemeldeten Benutzer zurück.
signedInMailUsers	Gibt die Anzahl der am E-Mail-Client angemeldeten Benutzer zurück.
productName	Gibt den Produktnamen des lizenzierten IVEs zurück.
productVersion	Gibt die Softwareversion des IVE-Systems zurück.

Tabelle 2: NetScreen-MIB-Objekte: Traps

Objekt	Beschreibung
iveLogNearlyFull	Eines der Protokolle (System, Benutzerzugriff oder Administratorenzugriff) ist zu 90% voll. Wenn dieses Trap gesendet wird, wird auch der Parameter `logFullPercent` (Protokolldatei ist zu % voll) gesendet.
iveLogFull	Eines der Protokolle (System, Benutzerzugriff oder Administratorenzugriff) ist restlos voll.
iveMaxConcurrentUsers SignedIn	Maximale Anzahl oder zulässige Anzahl von Benutzern ist gleichzeitig angemeldet, plus 10%.
iveTooManyFailedLogin Attempts	Für die angegebene IP-Adresse sind zu viele fehlgeschlagene Anmeldeversuche ausgeführt worden. Wird ausgelöst, wenn die Authentifizierung eines Benutzers im Verlauf einer Stunde 180-mal fehlschlägt. Nach dem Empfang dieser Meldung wird die IP-Adresse des Benutzers für 2 Minuten gesperrt, bevor seine Anmeldung wieder zulässig ist. Wenn dann der Anmeldevorgang des Benutzers innerhalb von 30 Minuten 90-mal fehlschlägt, wird seine IP-Adresse erneut gesperrt. Dieser Zyklus wird fortgesetzt, wobei der Zeitraum und die Anzahl fehlgeschlagener Anmeldeversuche jeweils halbiert wird. Im dritten Zyklus wird der Benutzer nach 45 fehlgeschlagenen Anmeldeversuchen innerhalb 15 Minuten gesperrt, im vierten Zyklus nach 23 fehlgeschlagenen Anmeldeversuchen innerhalb 8 Minuten usw. Wenn dieses Trap gesendet wird, wird auch der Parameter `blockedIP` (Quell-IP der Anmeldeversuche) gesendet.
externalAuthServer Unreachable	Ein externer Authentifizierungsserver beantwortet keine Authentifizierungsanforderungen. Wenn dieses Trap gesendet wird, wird auch der Parameter `authServerName` (Name des nicht erreichbaren Servers) gesendet.
iveStart	IVE wurde soeben eingeschaltet.
iveShutdown	IVE wurde soeben heruntergefahren.
iveReboot	IVE wurde soeben neu gestartet.

Tabelle 2: NetScreen-MIB-Objekte: Traps fortgesetzt

Objekt	Beschreibung
archiveServer Unreachable	IVE kann den konfigurierten FTP-Archivierungsserver nicht erreichen.
archiveServerLogin Failed	IVE kann sich nicht beim konfigurierten FTP-Archivierungsserver anmelden.
archiveFileTransfer Failed	IVE kann keine erfolgreiche Übertragung des Archivs auf den konfigurierten FTP-Archivierungsserver ausführen.

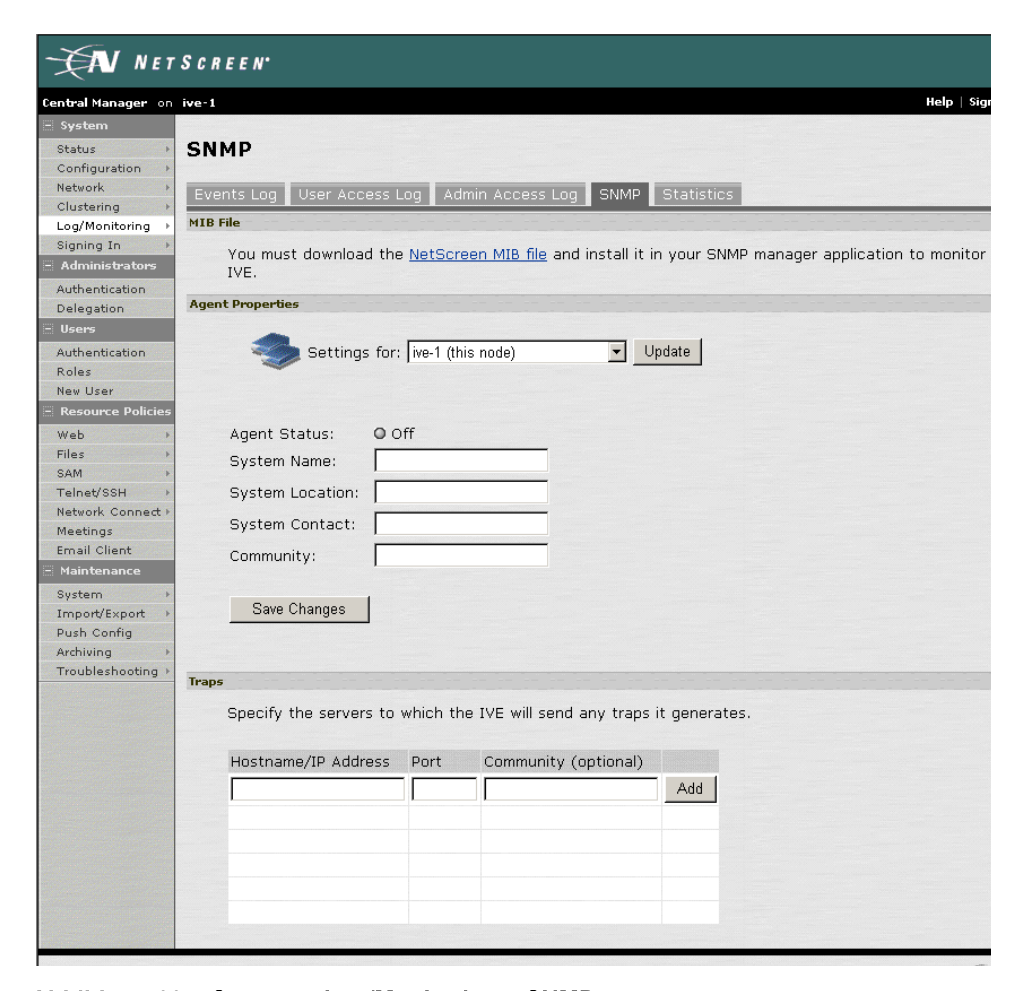


Abbildung 66: **System > Log/Monitoring > SNMP**

Registerkarte „Statistics“

☑ Anzeigen der Systemstatistik

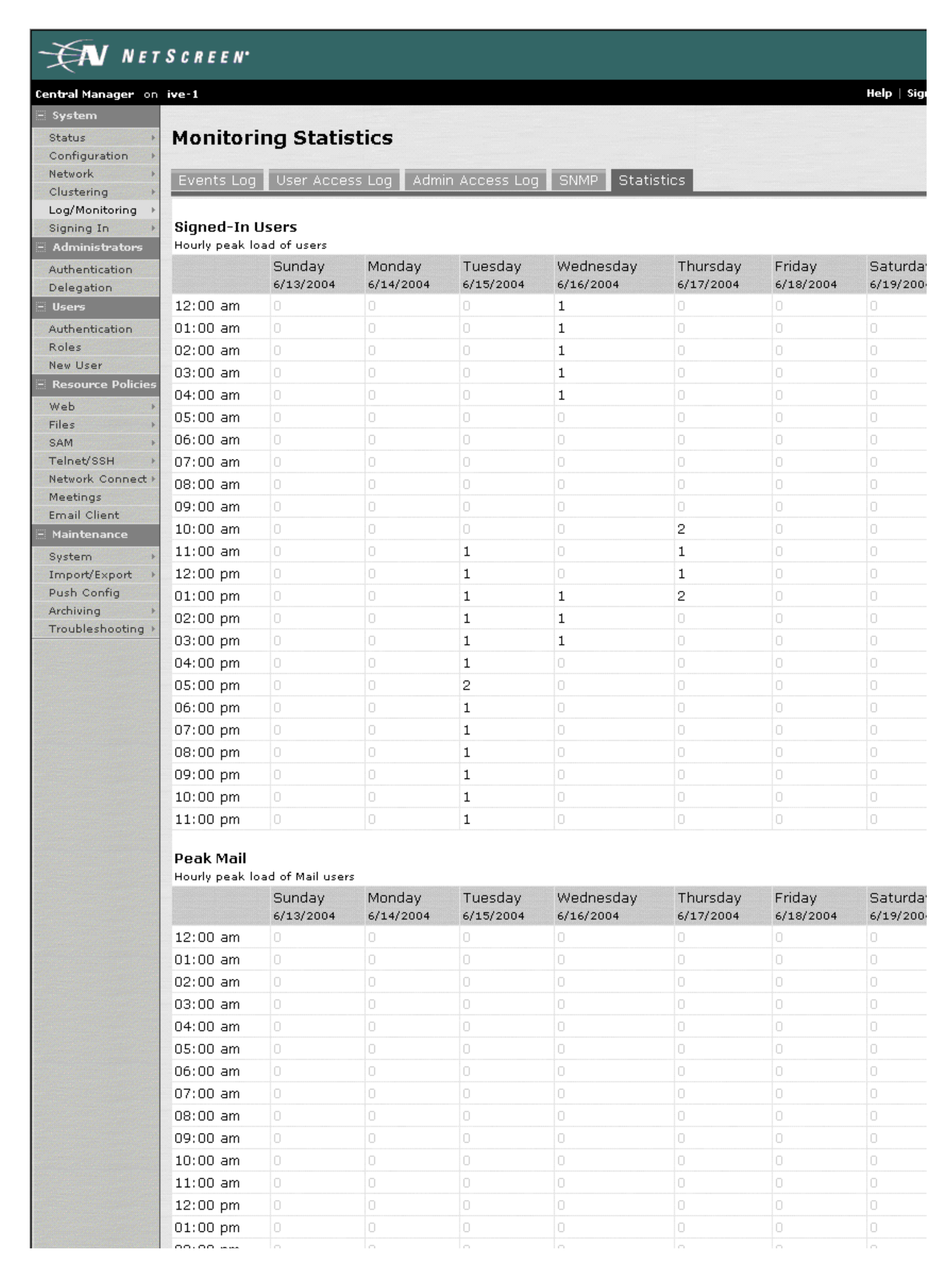
Das IVE protokolliert stündlich die folgenden Daten:

- Spitzenbelastung durch Webbenutzer
- Spitzenbelastung durch E-Mail-Benutzer
- Anzahl der URLs, auf die zugegriffen wird
- Anzahl der Dateien, auf die zugegriffen wird

Auf der Seite **Statistics** werden die Informationen für die letzten sieben Tage angezeigt. Diese Informationen werden einmal wöchentlich in das Systemprotokoll geschrieben. Beim Aktualisieren des IVE werden alle Statistiken gelöscht. Wenn Sie das System so konfigurieren, dass es stündlich die Statistik protokolliert, sind die alten Statistiken nach einer Aktualisierung immer noch in der Protokolldatei verfügbar.

So zeigen Sie die Systemstatistik an:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring > Statistics** aus.
2. Führen Sie auf der Seite einen Bildlauf durch, um alle vier Datenkategorien anzuzeigen.



	Sunday 6/13/2004	Monday 6/14/2004	Tuesday 6/15/2004	Wednesday 6/16/2004	Thursday 6/17/2004	Friday 6/18/2004	Saturda 6/19/200
12:00 am	0	0	0	1	0	0	0
01:00 am	0	0	0	1	0	0	0
02:00 am	0	0	0	1	0	0	0
03:00 am	0	0	0	1	0	0	0
04:00 am	0	0	0	1	0	0	0
05:00 am	0	0	0	0	0	0	0
06:00 am	0	0	0	0	0	0	0
07:00 am	0	0	0	0	0	0	0
08:00 am	0	0	0	0	0	0	0
09:00 am	0	0	0	0	0	0	0
10:00 am	0	0	0	0	2	0	0
11:00 am	0	0	1	0	1	0	0
12:00 pm	0	0	1	0	1	0	0
01:00 pm	0	0	1	1	2	0	0
02:00 pm	0	0	1	1	0	0	0
03:00 pm	0	0	1	1	0	0	0
04:00 pm	0	0	1	0	0	0	0
05:00 pm	0	0	2	0	0	0	0
06:00 pm	0	0	1	0	0	0	0
07:00 pm	0	0	1	0	0	0	0
08:00 pm	0	0	1	0	0	0	0
09:00 pm	0	0	1	0	0	0	0
10:00 pm	0	0	1	0	0	0	0
11:00 pm	0	0	1	0	0	0	0

	Sunday 6/13/2004	Monday 6/14/2004	Tuesday 6/15/2004	Wednesday 6/16/2004	Thursday 6/17/2004	Friday 6/18/2004	Saturda 6/19/200
12:00 am	0	0	0	0	0	0	0
01:00 am	0	0	0	0	0	0	0
02:00 am	0	0	0	0	0	0	0
03:00 am	0	0	0	0	0	0	0
04:00 am	0	0	0	0	0	0	0
05:00 am	0	0	0	0	0	0	0
06:00 am	0	0	0	0	0	0	0
07:00 am	0	0	0	0	0	0	0
08:00 am	0	0	0	0	0	0	0
09:00 am	0	0	0	0	0	0	0
10:00 am	0	0	0	0	0	0	0
11:00 am	0	0	0	0	0	0	0
12:00 pm	0	0	0	0	0	0	0
01:00 pm	0	0	0	0	0	0	0

Abbildung 67: System > Log/Monitoring > Statistics

Konfigurieren der Seite „Signing-in“

Die Seite **System > Signing-in** enthält die folgenden Registerkarten:

Auf der Seite **System > Signing-in** können Sie Folgendes durchführen:

Registerkarte „Sign-in Policies“

Anmelderichtlinien legen die URLs fest, die Benutzer und Administratoren für den Zugriff auf das IVE verwenden können. Bei der Konfiguration einer Anmelderichtlinie müssen Sie diese mindestens einem Bereich zuordnen. Es können sich dann nur Mitglieder des/der angegebenen Authentifizierungsbereiche(s) über den URL anmelden, der in der Richtlinie festgelegt ist. Sie können in der Anmelderichtlinie auch unterschiedliche Anmeldeseiten festlegen und sie unterschiedlichen URLs zuordnen.

So können Sie z. B. Anmelderichtlinien erstellen, die Folgendes angeben:

- Mitglieder des Bereichs „Partner“ können sich über folgende URLs beim IVE anmelden: `partner1.eigenefirma.com` und `partner2.eigenefirma.com`. Für Benutzer, die sich über den ersten URL anmelden, öffnet sich die Anmeldeseite „partner1“; für Benutzer, die sich über den zweiten URL anmelden, öffnet sich die Anmeldeseite „partner2“.

- Mitglieder der Bereiche „Lokal" und „Remote" können sich über den folgenden URL beim IVE anmelden: `mitarbeiter.eigenefirma.com`. Bei der Anmeldung wird die Anmeldeseite „Mitarbeiter" geöffnet.
- Mitglieder des Bereichs „Admin Users" können sich über den folgenden URL beim IVE anmelden: `zugriff.eigenefirma.com/super`. Bei der Anmeldung wird die Anmeldeseite „Administratoren" geöffnet.

Beim Festlegen von Anmelderichtlinien können Sie verschiedene Hostnamen verwenden (z. B. `partner.eigenefirma.com` und `mitarbeiter.eigenefirma.com`) oder verschiedene Pfade (z. B. `eigenefirma.com/partner` und `eigenefirma.com/mitarbeiter`), um zwischen den URLs zu unterscheiden.

Wichtig: Wenn Sie die URLs anhand von Hostnamen unterscheiden, müssen Sie jedem Hostnamen ein eigenes Zertifikat zuordnen oder ein Platzhalterzertifikat anhand von Optionen auf der Seite **System > Configuration > Certificates > Server Certificates** in das IVE hochladen.

☑ Erstellen und Konfigurieren von Anmelderichtlinien

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Sign-in Policies** aus.
2. Um eine neue Anmelderichtlinie zu erstellen, klicken Sie auf **New**. Wenn Sie eine vorhandene Richtlinie bearbeiten möchten, klicken Sie auf einen URL in der Spalte **Administrator URLs** oder **User URLs**.

Hinweis: Wenn Sie über eine Secure Meeting-Lizenz verfügen, wird die Richtlinie ***/meeting** in der Spalte **User URLs** angezeigt. Die Secure Meeting-Benutzern angezeigte Standardanmeldeseite können Sie nur mit dieser Richtlinie bearbeiten. Sie können jedoch nicht den URL ändern, über den die Benutzer auf eine Konferenz zugreifen oder eine benutzerdefinierte Anmeldeseite für Konferenzen erstellen.

---

3. Wählen Sie **Users** oder **Administrators** aus, um anzugeben, welcher Typ von Benutzer sich mithilfe dieser Richtlinie beim IVE anmelden kann.

4. Geben Sie im Feld **Sign-in URL** den URL ein, die Sie der Richtlinie zuordnen möchten.
   - Um anzugeben, dass alle Administrator-URLs innerhalb des festgelegten Bereichs bzw. der festgelegten Bereiche die Anmeldeseite verwenden müssen, geben Sie ***/admin** ein.
   - Um anzugeben, dass alle Endbenutzer-URLs innerhalb des festgelegten Bereichs bzw. der festgelegten Bereiche die Anmeldeseite verwenden müssen, geben Sie ***/** ein.

Hinweis: Im Hostnamenabschnitt des URLs können Sie nur Platzhalterzeichen (*) verwenden. Das IVE erkennt keine Platzhalter im URL-Pfad.

---

5. Geben Sie unter **Description** eine Beschreibung für die Richtlinie ein (optional).
6. Wählen Sie unter **Sign-in page** eine Anmeldeseite aus. Sie können die Standardseite für das IVE auswählen, eine Variation der Standardanmeldeseite oder eine benutzerdefinierte Seite, die Sie mithilfe der Funktion „Customizable UI“ erstellen. Weitere Informationen finden Sie unter „Registerkarte „Sign-in Page““ auf Seite 274.
7. Legen Sie unter **Authentication realm** fest, welche Bereiche der Richtlinie zugeordnet sein sollen und wie Benutzer und Administratoren unter den Bereichen auswählen sollen. Wenn Sie Folgendes auswählen:
   - **User types the realm name**

     Die Anmelderichtlinie wird allen Authentifizierungsbereichen zugeordnet, das IVE stellt jedoch keine Bereichsliste bereit, aus der ein Benutzer oder Administrator auswählen kann. Stattdessen muss der Benutzer oder Administrator seinen Bereichsnamen manuell auf der Anmeldeseite eingeben.
   - **User picks from a list of authentication realms**

     Die Anmelderichtlinie ist nur dem von Ihnen gewählten Authentifizierungsbereich zugeordnet. Das IVE zeigt dem Benutzer oder Administrator diese Bereichsliste bei der Anmeldung am IVE an und ermöglicht die Auswahl eines in der Liste aufgeführten Bereichs. (Wenn dem URL nur ein einziger Bereich zugeordnet ist, zeigt das IVE keine Dropdownliste von Bereichen an. Stattdessen verwendet es automatisch den von Ihnen festgelegten Bereich.)
8. Klicken Sie auf **Save Changes**.

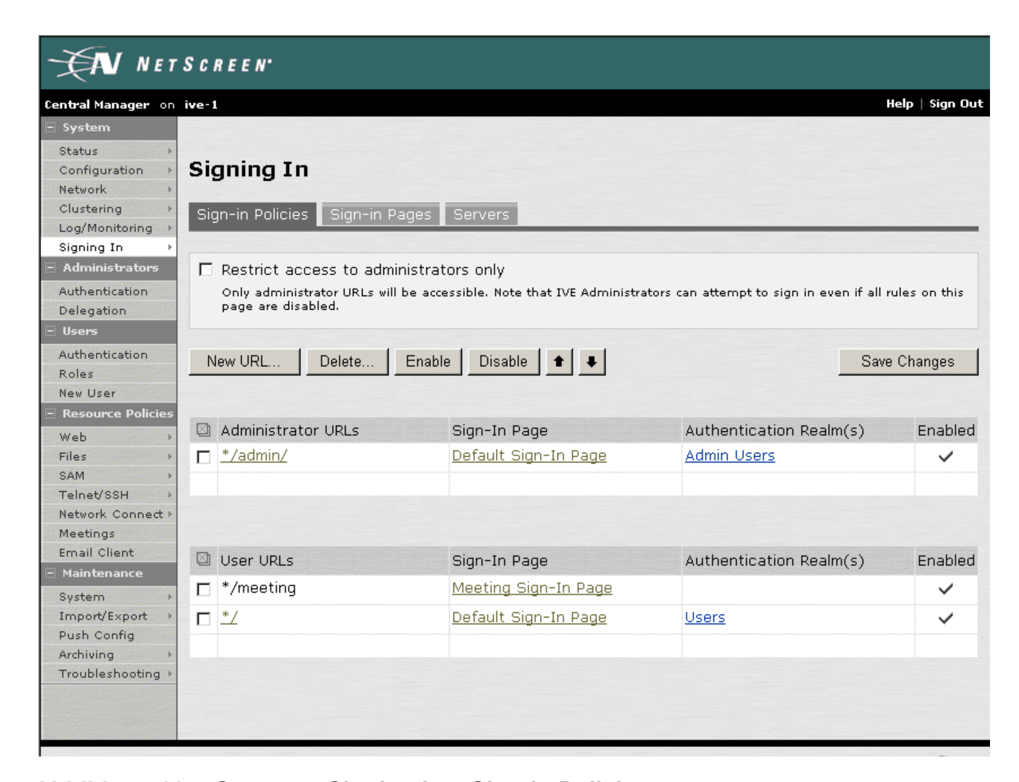


Abbildung 68: **System > Signing In > Sign-in Policies**

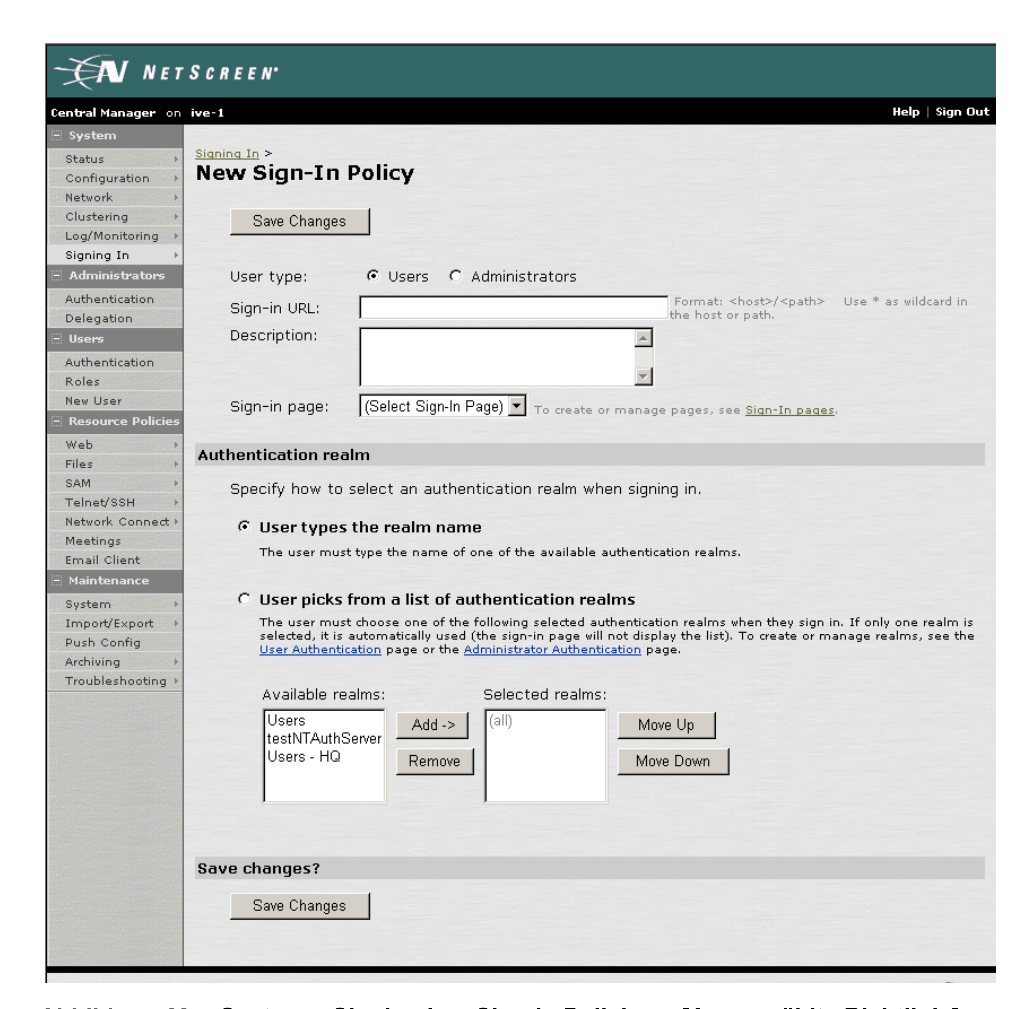


Abbildung 69: System > Signing In > Sign-in Policies > [Ausgewählte Richtlinie]

☑ Festlegen der Auswertungsreihenfolge von Anmelderichtlinien

Das IVE wertet die Anmelderichtlinien für Administratoren in der gleichen Reihenfolge aus, in der sie auf der Seite **Sign-in Policies** aufgeführt sind, und wertet dann die Anmelderichtlinien für Benutzer aus. Wenn es einen exakt übereinstimmenden URL findet, bricht es die Auswertung ab und öffnet die entsprechende Anmeldeseite für den Administrator bzw. Benutzer. Sie können z. B. zwei Administrator-Anmelderichtlinien mit zwei verschiedenen URLs festlegen:

- Die erste Richtlinie verwendet den URL `*/admin` und ordnet die Standardanmeldeseite für Administratoren zu.
- Die zweite Richtlinie verwendet den URL `eigenefirma.com/admin` und ordnet eine benutzerdefinierte Anmeldeseite für Administratoren zu.

Wenn Sie die Richtlinien in dieser Reihenfolge auf der Seite **Sign-in Policies** aufführen, wertet das IVE die zweite Richtlinie niemals aus bzw. verwendet sie nie, da der erste URL den zweiten einschließt. Selbst bei der Anmeldung eines Administrators über den URL `eigenefirma.com/admin` zeigt das IVE die Standardanmeldeseite für Administratoren an. Wenn Sie die Richtlinien hingegen in umgekehrter Reihenfolge aufführen, zeigt das IVE die benutzerdefinierte Anmeldeseite allen Administratoren an, die über den URL `eigenefirma.com/admin` auf das IVE zugreifen.

Das IVE akzeptiert nur Platzhalterzeichen im Hostnamenabschnitt des URLs und ordnet den URL anhand des exakten Pfades zu. Sie können z. B. zwei Administrator-Anmelderichtlinien mit zwei verschiedenen URL-Pfaden festlegen:

- Die erste Richtlinie verwendet den URL `*/marketing` und ordnet eine benutzerdefinierte Anmeldeseite für die gesamte Marketingabteilung zu.
- Die zweite Richtlinie verwendet den URL `*/marketing/joe` und ordnet eine benutzerdefinierte Anmeldeseite zu, die ausschließlich für den Mitarbeiter „Joe" der Marketingabteilung vorgesehen ist.

Wenn Sie die Richtlinien auf der Seite **Sign-in Policies** in dieser Reihenfolge aufführen, zeigt das IVE die benutzerdefinierte Anmeldeseite für Joe immer dann an, wenn Joe über den URL `eigenefirma.com/marketing/joe` auf das IVE zugreift. Joe wird die Marketinganmeldeseite nicht angezeigt, obwohl sie als erste aufgeführt und ausgewertet wird, da der Pfadabschnitt seines URL nicht genau mit dem URL übereinstimmt, der in der ersten Richtlinie definiert ist.

So ändern Sie die Reihenfolge, in der die Anmelderichtlinien für Administratoren ausgewertet werden:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Sign-in Policies** aus.
2. Wählen Sie eine Anmelderichtlinie aus der Liste **Administrator URL** aus.
3. Ändern Sie die Position der Richtlinie in der Liste mithilfe der Pfeile nach oben oder nach unten.
4. Klicken Sie auf **Save Changes**.

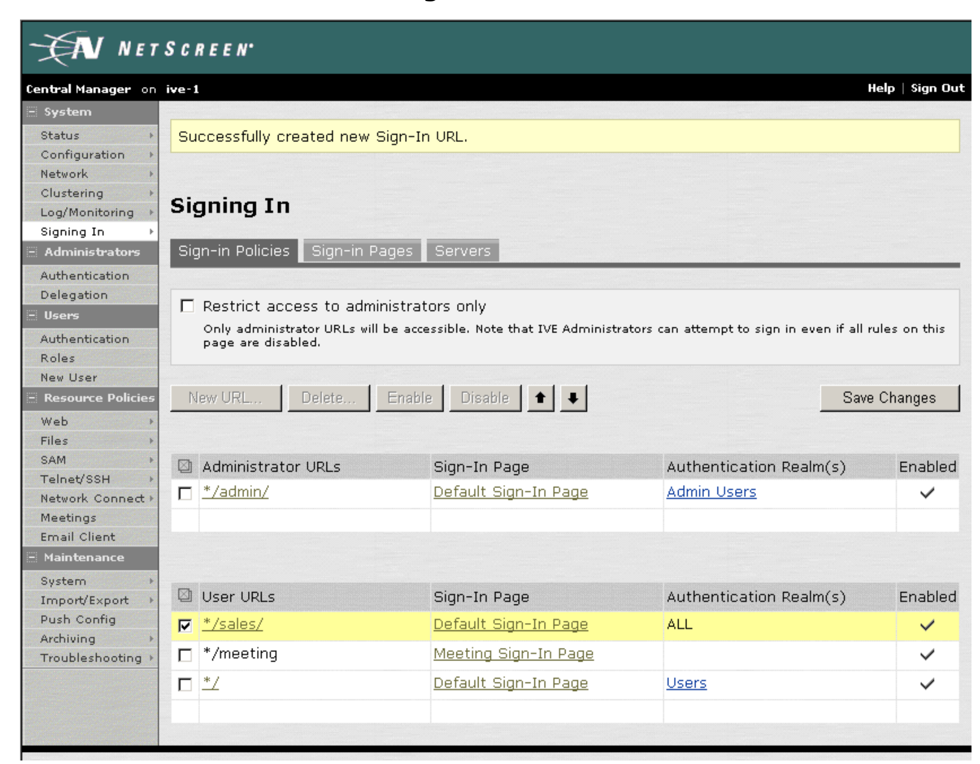


Abbildung 70: **System > Signing In > Sign-in Policies (Änderung der Reihenfolge)**

☑ Aktivieren und Deaktivieren von Anmelderichtlinien

So aktivieren und deaktivieren Sie Anmelderichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Sign-in Policies** aus.
2. So gehen Sie für die Aktivierung oder Deaktivierung vor:
   - **Einzelne Richtlinie** – Aktivieren Sie das Kontrollkästchen neben der Richtlinie, die Sie ändern möchten, und klicken Sie dann auf **Enable** oder **Disable**.
   - **Alle Benutzerrichtlinien** – Aktivieren oder deaktivieren Sie das Kontrollkästchen **Restrict access to administrators only**.

Registerkarte „Sign-in Page“

Eine Anmeldeseite legt die benutzerdefinierten Eigenschaften der Willkommensseite des Benutzers fest, wie etwa Begrüßungstext, Hilfetext, Logo, Kopf- und Fußbereich. Das IVE ermöglicht es Ihnen, Benutzern und Administratoren zwei Arten von Anmeldeseiten anzuzeigen.

- **Standardanmeldeseiten**

  Die Standardanmeldeseiten sind von Juniper Networks vorgegeben und in allen Versionen des IVE enthalten. Beachten Sie, dass auch die Seiten, die über die Registerkarte **System > Signing In > Sign-in Page** geändert werden, als Standardanmeldeseiten zählen. Weitere Informationen finden Sie unter „Standardanmeldeseiten“ auf Seite 275.

- **Benutzerdefinierte Anmeldeseiten**

  Benutzerdefinierte Anmeldeseiten sind THTML-Seiten, die Sie mithilfe des Template Toolkit erstellen und in Form einer archivierten ZIP-Datei in das IVE hochladen. Die Erstellung von benutzerdefinierten Anmeldeseiten ist eine lizenzierte Funktion, die es Ihnen ermöglicht, anstelle der geänderten IVE-Anmeldeseite eigene Seiten zu verwenden. Weitere Informationen finden Sie unter „Benutzerdefinierte Anmeldeseiten“ auf Seite 278.

Standardanmeldeseiten

Im IVE werden folgende Standardanmeldeseiten bereitgestellt:

- **Standardanmeldeseite**

  In der Standardeinstellung ist das IVE so konfiguriert, dass Benutzern diese Seite angezeigt wird, wenn sie sich beim IVE anmelden.

- **Anmeldeseite für Konferenzen**

  Benutzern wird vom IVE diese Seite angezeigt, wenn sie sich bei einer Konferenz anmelden. Diese Seite ist nur verfügbar, wenn Sie im IVE eine Secure Meeting-Lizenz installieren.

Auf der Registerkarte **Sign-In Pages** können Sie diese Seiten bearbeiten bzw. eine neue IVE-Standardanmeldeseite mit benutzerdefiniertem Text, Logo, Fehlermeldungstext und benutzerdefinierten Farben erstellen.

☑ Erstellen oder Bearbeiten einer Standardanmeldeseite

So erstellen oder bearbeiten Sie eine Standardanmeldeseite:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Sign-in Pages** aus.
2. Gehen Sie dabei folgendermaßen vor:
   - **Erstellen einer neuen Seite** – Klicken Sie auf **New Page**.
   - **Bearbeiten einer vorhandenen Seite** – Wählen Sie die entsprechende Verknüpfung für die zu bearbeitende Seite aus.
3. Geben Sie einen Namen ein, um die Seite zu bezeichnen.
4. Ändern Sie im Abschnitt **Custom Text** den für die verschiedenen Fensterbeschriftungen verwendeten Standardtext nach Bedarf. Wenn Sie im Feld **Instructions** Text hinzufügen, ist zu beachten, dass das Formatieren von Text und Hinzufügen von Verknüpfungen anhand der folgenden HTML-Tags erfolgen kann: `<i>`, `<b>`, `<br>`, `<font>` und `<a href>`. Allerdings schreibt das IVE Verknüpfungen auf der Anmeldseite (aufgrund der noch nicht erfolgten Benutzerauthentifizierung) nicht neu. Folglich sollten Sie nur Verweise auf externe Sites erstellen. Verknüpfungen zu Sites hinter einer Firewall funktionieren nicht.
5. Legen Sie im Abschnitt **Header** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Seitenkopf fest.
6. Ändern Sie im Abschnitt **Custom Error Messages** den Standardtext, der Benutzern angezeigt wird, wenn bei diesen Zertifikatsfehler auftreten. (Nicht für die Secure Meeting-Anmeldeseite verfügbar.)

7. Um Benutzern benutzerdefinierte Hilfeinformationen oder zusätzliche Anweisungen bereitzustellen, wählen Sie **Show Help Button** aus, geben Sie eine Beschriftung für die Schaltfläche ein, und geben Sie eine HTML-Datei an, die in das IVE hochgeladen werden soll. Beachten Sie, dass im IVE keine Bilder und anderen Inhalte angezeigt werden, auf die in dieser HTML-Seite verwiesen wird. (Nicht für die Secure Meeting-Anmeldeseite verfügbar.)
8. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden.

Hinweis: Klicken Sie auf **Restore Factory Defaults**, um die Darstellung der Anmeldeseite, der IVE-Startseite für Benutzer und der Webkonsole zurückzusetzen.

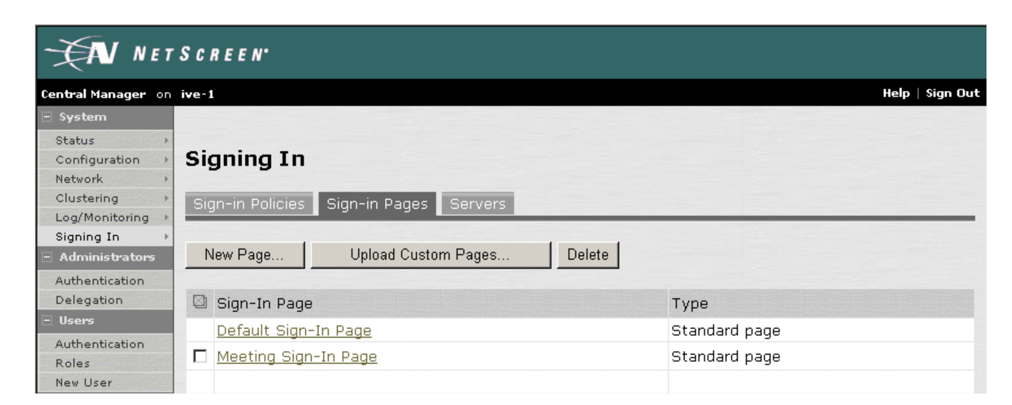


Abbildung 71: System > Signing In > Sign In Pages

NETSCREEN
Central Manager
Help | Sign Out

System
- Status
- Configuration
- Network
- Clustering
- Log/Monitoring
- Signing In

Administrators
- Authentication
- Delegation

Users
- Authentication
- Roles
- New User

Resource Policies
- Web
- Files
- SAM
- Telnet/SSH
- Network Connect
- Meetings
- Email Client

Maintenance
- System
- Import/Export
- Push Config
- Archiving
- Troubleshooting

Signing In >

Default Sign-In Page

Name: Default Sign-In Page — Label to reference the sign-in page.

Custom text

Welcome message:

Portal name:

Username: Username

Password: Password

Realm: Realm — This prompt appears when the sign in page supports more than one realm.

Sign In button: Sign In

Instructions: Please sign in to begin your secure session.

This text appears on the right-hand side of the sign-in page. You can use <b>,
, and <a href> tags to format the text.

Sign Out message: Your session has ended. — Text appears in message box when user signs out

Sign In link text: Click here to sign in again — Text appears as link to sign in page when user signs out

Header appearance

Current appearance: NETSCREEN

Logo image: Browse... — Recommended size: Less than 40 pixels tall and 10KB.

Background color: #666666 — Select from palette or type hexadecimal RGB

Custom error messages

Missing certificate: To sign in, your machine must have a client-side certificate. Please contact your system administrator.

This message appears when the user does not have a required client-side certificate.

Invalid certificate: Your client-side certificate is invalid. Please contact your system administrator.

This message appears when the user does not have a valid required client-side certificate.

☑ Show Help button

If you want to provide users with more information regarding sign-in requirements, you can display a Help button that links to a custom HTML file.

Help button: Help — Displayed only if Help Button is enabled.

HTML file: Browse... — Note that images and other external content will not be displayed.

Save changes?

Abbildung 72: System > Signing In > Sign In Pages > [Ausgewählte Seite]

Benutzerdefinierte Anmeldeseiten

Mit der Funktion der benutzerdefinierten Anmeldeseiten können Sie das Erscheinungsbild der Seiten für Authentifizierungs-Vorabprüfungen und Kennwortverwaltung personalisieren, die das IVE für Administratoren und Endbenutzer bereitstellt. Mit dieser Funktion können eine Reihe von Seiten angepasst werden. Eine vollständige Liste finden Sie in Anhang E.: auf Seite 613.

Hinweis: Die IVE-Standardseiten, die Benutzern nach der Authentifizierung angezeigt werden, z. B. die Lesezeichenseite, die Dateinavigationsseiten oder die Seiten der Endbenutzerhilfe, können nicht angepasst werden. Sie können jedoch auf der Registerkarte **Users > Roles > [Rolle] > General > UI Options** über die Option **Start page URL** Benutzer zu Ihrer eigenen benutzerdefinierten Seite und nicht zur IVE-Startseite weiterleiten. Von dort aus können Sie für Benutzer Verknüpfungen zu beliebigen Seiten erstellen. Durch Verwenden dieser Option in Verbindung mit der Funktion für benutzerdefinierte Anmeldeseiten können Sie dafür sorgen, dass Benutzern nur wenige IVE-Standardseiten angezeigt werden.

Führen Sie zum Erstellen und Aktivieren Ihrer benutzerdefinierten Seiten die folgenden Schritte aus:

☑ Erstellen benutzerdefinierter Anmeldeseiten

Juniper Networks lässt benutzerdefinierte Seiten mithilfe des Template Toolkit-Verarbeitungssystems darstellen[1]. Dieses System bietet Ihnen die Möglichkeit, die Template Toolkit-Sprache zu verwenden, um Ihren benutzerdefinierten Seiten dynamisches Verhalten hinzuzufügen (wie unter „Informationen zur Template Toolkit-Sprache“ auf Seite 614 beschrieben). Das Aktivieren Ihrer Seiten für die Zusammenarbeit mit diesem System ist einfach: Verwenden Sie beim Anpassen der IVE-Seiten Ihren bevorzugten HTML-Editor, um auf Grundlage der bereitgestellten Vorlagen HTML, CSS und JavaScript zu erstellen. Sie können Ihren Seiten bei Bedarf auch mithilfe der Template Toolkit-Sprache Bedingungsanweisungen, Schleifenkonstruktionen und dynamisches Verhalten hinzufügen.

1. Erstellung und Unterstützung der benutzerdefinierten Anmeldeseiten erfolgt mit Version 2.09 des Template Toolkits.

Anschließend müssen die Dateien als Vorlagendateien (THTML) gespeichert werden. (Wenn Sie beispielsweise die IVE-Standardanmeldeseite ändern möchten, müssen Sie diese als `LoginPage.thtml` und nicht als `LoginPage.html` speichern.) Auf diese Weise werden die benutzerdefinierten Seiten vom IVE erkannt und an Stelle der eigenen HTML-Standardseiten verwendet.

Beim Erstellen einer benutzerdefinierten Seite für das IVE wird dringend empfohlen, auf die mit dem IVE bereitgestellten Vorlagen zurückzugreifen. In diesen Vorlagen sind alle erforderlichen Variablen und Formularfelder sowie sämtliches JavaScript enthalten, die über die benutzerdefinierten Seiten an das IVE weitergeleitet werden müssen. Darüber hinaus enthalten die Vorlagen in den ZIP-Dateien optionalen Code, der Sie beim Erstellen der Seiten unterstützen kann. Weitere Informationen finden Sie in Anhang E.: auf Seite 613.

Beachten Sie beim Erstellen benutzerdefinierter Seiten Folgendes:

- Sie müssen über praktische Erfahrung mit HTML und JavaScript verfügen, um benutzerdefinierte IVE-Seiten zu erstellen.
- Benutzer können sich nicht beim IVE anmelden, wenn in Ihren Vorlagen nicht alle erforderlichen Daten enthalten sind. Es wird deswegen dringend empfohlen, beim Erstellen der Seiten die Beispielvorlagen zu verwenden.
- Beim Erstellen einer Verknüpfung mit einer Ressource, die sich nicht auf dem IVE befindet, müssen Sie den absoluten Ressourcenpfad mit vorangestelltem „http://“ verwenden. Beispiel:

  ```
  http://www.google.com
  ```

- Beim Erstellen eines Verweises auf eine Ressource in Ihrer ZIP-Datei können Sie mithilfe von Standard-HTML auf Dateien mit den Erweiterungen .txt, .html, .gif, .jpg, .js, .pdf, .css, .class, .jar und .cab verweisen, oder Sie können die Template Toolkit-Sprache verwenden, um Verweise auf Dateien mit der Erweiterung .thtml zu erstellen. Beispiel:

  ```
  <a href= „link.gif“>Click Here</a>

  <% INCLUDE LoginPage.thtml %>
  ```

- Wenn Sie einen Verweis auf ein übergeordnetes Verzeichnis einer Ressource in der ZIP-Datei erstellen, können Sie die Konvention „..“ oder die Variable `<% Home %>` verwenden, um einen Verweis auf das oberste Verzeichnis zu erstellen. Beispiel:

  ```
  <% Home %>/images/logo.gif

  ../images/logo.gif
  ```

- Wenn mehrere Sprachen unterstützt werden sollen, müssen Sie für jede unterstützte Sprache separate Seiten erstellen, die in eigenen ZIP-Dateien (z. B. **französisch.zip** oder **englisch.zip**) gespeichert werden müssen. Jede ZIP-Datei wird einem eigenen URL zugeordnet, und die Benutzer müssen darauf hingewiesen werden, sich je nach gewünschter Sprache über den entsprechenden URL anzumelden.
- Die IVE-Standardseiten, die Benutzern nach der Authentifizierung angezeigt werden, z. B. die Lesezeichenseite, die Dateinavigationsseiten oder die Seiten der Endbenutzerhilfe, können nicht angepasst werden.
- Ab Version 4.1 ist jede benutzerdefinierte Vorlage des IVE mit einer Versionsnummer versehen. Diese Nummer darf nicht geändert werden.

So greifen Sie auf die Beispieldaten des IVE zu:

1. Melden Sie sich als Administrator bei der Webkonsole an.
2. Wählen Sie **System > Signing In > Sign-in Pages** aus. (**Abbildung 72** auf Seite 277)
3. Klicken Sie auf **Upload Custom Pages**.
4. Wählen Sie eine der folgenden Dateien zum Herunterladen aus:
   - Sample
   - SoftID
   - Kiosk
5. Speichern Sie diese in einem lokalen Verzeichnis.

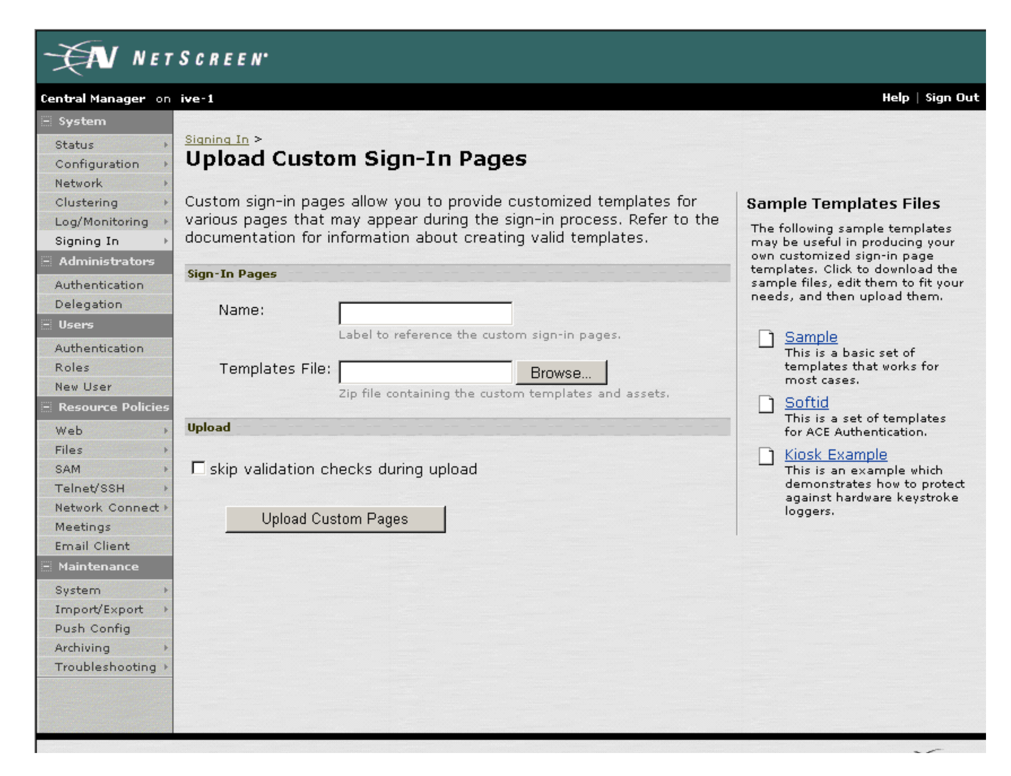


Abbildung 73: **System > Signing In > Sign In Pages > Upload Custom Pages**

☑ Archivieren von Vorlagen in einer ZIP-Datei

Nach dem Erstellen benutzerdefinierter Seiten müssen alle Vorlagen und unterstützenden Bilder, Stylesheets, JavaScript-Dateien und Applets in einer ZIP-Datei archiviert werden. Beim Erstellen eines Archivs sollten Sie Folgendes beachten:

- CGI-Dateien können in der ZIP-Datei nicht gespeichert werden. Andernfalls wird das Hochladen vom IVE verweigert.
- Die kombinierte Gesamtdateigröße aller ZIP-Dateien, die in das IVE hochgeladen werden, darf nicht mehr als 7,5 MB betragen.
- Sämtliche Vorlagendateien (.thtml) müssen in das oberste Verzeichnis der erweiterten ZIP-Datei übernommen werden.
- Die Dateien `LoginPage.thtml`, `ExceedConcurrent.thtml`, `SSL.thtml` und `Logout.thtml` müssen sich auf der Stammebene des Archivs befinden, selbst wenn nicht alle diese Dateien vom IVE verwendet werden sollen. Andernfalls wird das Hochladen vom IVE verweigert.

- Wenn Sie keine optionalen Seiten (z. B. `SelectRoles.thtml` oder `PleaseWait.thtml`) in die ZIP-Datei einfügen, verwendet das IVE stattdessen seine eigenen Standardseiten, um sicherzustellen, dass den Benutzern alle Funktionen zur Verfügung stehen. Aus Gründen der Einheitlichkeit fügt das IVE jedoch alle anwendbaren Headerelemente, die Sie für die Standardanmeldeseite festgelegt haben, in die eigenen Standardseiten ein. Benutzerdefinierte Headerelemente können Sie in der Webkonsole über die Einstellungen auf der Registerkarte **System > Signing In > Sign-in Pages** definieren.

☑ Hochladen von ZIP-Dateien mit benutzerdefinierten Anmeldeseiten in das IVE

Nach dem Archivieren der Vorlagen und unterstützenden Dateien in einer ZIP-Datei müssen Sie die ZIP-Datei in das IVE hochladen.

So laden Sie die ZIP-Datei in das IVE hoch:

1. Melden Sie sich als Administrator bei der Webkonsole an.
2. Wählen Sie **System > Signing In > Sign-in Pages** aus.
3. Klicken Sie auf **Upload Custom Pages**. (**Abbildung 73** auf Seite 281)
4. Geben Sie einen Namen ein, um die ZIP-Datei im IVE zu bezeichnen.

   Wichtig: Wenn Sie einen Namen wählen, der mit dem Namen einer bereits im IVE vorhandenen ZIP-Datei identisch ist, überschreibt das IVE das bestehende Archiv mit dem neuen Archiv, sodass nur die aktuelle Version gespeichert wird.

5. Navigieren Sie im Browser zu der ZIP-Datei, die Ihre benutzerdefinierte(n) Seite(n) enthält.
6. Aktivieren Sie das Kontrollkästchen **skip validation checks during upload**, wenn das IVE nicht überprüfen soll, ob in den Vorlagen alle erforderlichen Variablen enthalten sind. Eine Liste der erforderlichen Variablen finden Sie in den Kommentaren der IVE-Beispielvorlagen sowie in den Beschreibungen in Anhang E.: auf Seite 613. Das IVE führt Gültigkeitsüberprüfungen durch, nachdem Sie die Datei in das IVE hochgeladen haben und bevor Sie sie im angegebenen Verzeichnis auf dem Server speichern.

   Wichtig: Es wird empfohlen, diese Option nur dann zu aktivieren, wenn Sie in einer Nicht-Produktionsumgebung Schnelltests ausführen.

7. Klicken Sie auf **Save Changes**.

☑ Zuweisen der ZIP-Datei mit benutzerdefinierten Anmeldeseiten zu einem URL

Nach dem Hochladen der ZIP-Datei mit den Anmeldeseiten in das IVE müssen Sie sie einem Anmelde-URL zuordnen.

So weisen Sie die ZIP-Datei einem Anmelde-URL zu:

1. Melden Sie sich als Administrator bei der Webkonsole an.
2. Wählen Sie **System > Signing In > Sign-in Policies aus. (Abbildung 68** auf Seite 270)
3. Klicken Sie auf den URL, der den benutzerdefinierten Seiten zugeordnet werden soll.
4. Wählen Sie aus der Liste **Sign-in page** den im vorigen Abschnitt festgelegten Namen aus.
5. Klicken Sie auf **Save Changes**.

☑ Bestätigen der Funktionsfähigkeit der benutzerdefinierten Seiten

Um zu bestätigen, dass Ihre benutzerdefinierten Seiten vom IVE verwendet werden, melden Sie sich über den im vorigen Abschnitt angegebenen URL an, und bestätigen Sie, dass Sie die Seiten anzeigen können.

Registerkarte „Server“

Authentifizierungsserver authentifizieren Anmeldeinformationen der Benutzer, während Autorisierungsserver Benutzerinformationen bereitstellen, die das IVE zur Ermittlung von Benutzerberechtigungen im System verwendet. Sie können z. B. eine Zertifikatserverinstanz angeben, die Benutzer anhand ihrer clientseitigen Zertifikatsattribute authentifiziert, und dann eine LDAP-Serverinstanz erstellen, die Benutzer anhand der Werte autorisiert, die in einer Zertifikatsperrliste (Certificate Revocation List, CRL) aufgeführt sind. Weitere Informationen zu Authentifizierungsservern finden Sie unter „Authentifizierungsserver“ auf Seite 35.

☑ Definieren einer Authentifizierungsserverinstanz

So definieren Sie eine Serverinstanz:

1. Geben Sie Einstellungen für die individuelle Serverinstanz an. Anweisungen hierfür finden Sie unter:
   - Konfigurieren einer ACE/Serverinstanz (Seite 287)
   - Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz (Seite 293)
   - Konfigurieren einer Instanz eines anonymen Servers (Seite 297)
   - Konfigurieren einer Zertifikatserverinstanz (Seite 299)
   - Konfigurieren einer LDAP-Serverinstanz (Seite 303)
   - Konfigurieren einer lokalen IVE-Server-Instanz (Seite 309)
   - Konfigurieren einer Netegrity SiteMinder-Instanz321
   - Konfigurieren einer NIS-Serverinstanz (Seite 315)
   - Konfigurieren einer RADIUS-Serverinstanz (Seite 317)

   Hinweis: Beachten Sie bei der Auswahl des Servertyps Folgendes:
   - Sie können nur eine ACE- und eine RADIUS-Serverinstanz pro IVE erstellen.
   - Sie können den Active Directory-Server mit folgenden Protokollen authentifizieren:
     - **NTLM-Protokoll** – Wählen Sie **Active Directory/Windows NT Domain** Seite 293 aus.
     - **LDAP-Protokoll** – Wählen Sie **LDAP Server** Seite 303 aus.
   - Wenn Sie eine Serverinstanz zum Authentifizieren von Benutzeradministratoren erstellen Seite 309, müssen Sie **IVE Authentication** auswählen.
2. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll Seite 379.
3. Wenn Sie den lokalen IVE-Authentifizierungsserver konfigurieren, müssen Sie lokale Benutzerkonten festlegen. Anweisungen hierfür finden Sie auf Seite 309.

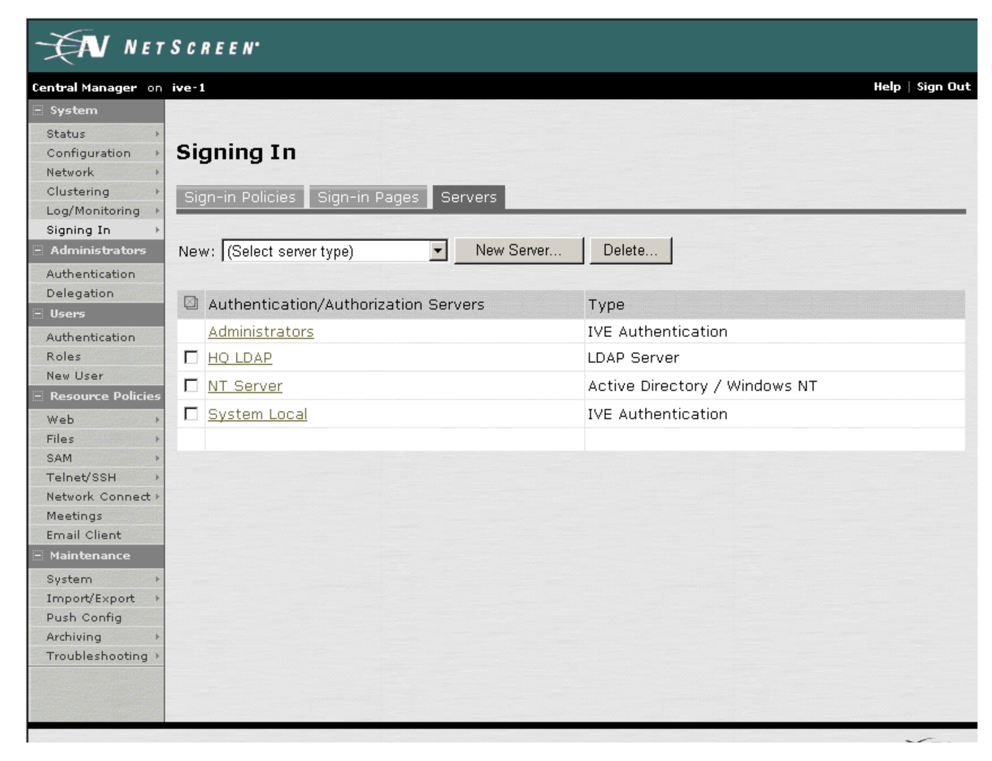


Abbildung 74: **System > Signing In > Servers**

Konfigurieren einer ACE/Serverinstanz

Die folgenden Themen werden behandelt:

ACE/Server – Übersicht

Wenn die Benutzerauthentifizierung über einen RSA ACE/Server erfolgt, können sich Benutzer mit zwei Methoden anmelden:

- **Unter Verwendung der IVE-Standardanmeldeseite:**
  Der Benutzer wechselt zur Standardanmeldeseite für das IVE, und gibt dann den Benutzernamen und das Kennwort ein (bestehend aus der Kombination von PIN und dem aktuellen Wert des RSA SecurID-Hardware- oder Softwaretokens). Das IVE leitet diese Anmeldeinformationen des Benutzers dann an ACE/Server weiter.
- **Unter Verwendung der RSA SecurID-Authentifizierungsseite:**
  Wenn der Benutzer RSA SecurID-Software im System installiert hat, kann er unter Verwendung des folgenden URL-Formats auf die Seite **RSA SecurID Authentication** wechseln:
  `https://IVE/login/ServerInstanz` und Eingabe der PIN. (In Abhängigkeit von der RSA-Konfiguration muss der Benutzer möglicherweise auch den Benutzernamen eingeben.) Wenn die IVE-Appliance die Gültigkeit der Anmeldeanforderung bestätigt hat, kann die RSA SecurID-Software einen Tokenwert transparent über die IVE-Appliance an ACE/Server weitergeben.

Wenn ACE/Server den Benutzer authentifiziert hat, wird der Zugriff auf die IVE-Appliance gewährt. Andernfalls führt ACE/Server folgende Aktionen aus:

- **Verweigern des Benutzerzugriffs auf das System**
  wenn die Anmeldeinformationen des Benutzers nicht erkannt wurden.
- **Weiterleiten des Benutzers an die IVE-Standardanmeldeseite**
  wenn der Benutzer versucht, sich auf der Seite **RSA SecurID Authentication** auf einem Computer anzumelden, auf dem die SecurID-Software nicht installiert ist.

- **Auffordern des Benutzers, eine neue PIN zu erstellen (New PIN-Modus)**
  wenn der Benutzer sich erstmals bei IVE anmeldet. (Dem Benutzer werden je nach verwendetem Anmeldeverfahren unterschiedliche Aufforderungen angezeigt. Bei Anmeldung über die Seite **RSA SecurID Authentication** werden die RSA-Aufforderungen zum Erstellen einer neuen PIN angezeigt. Andernfalls werden die IVE-Aufforderungen angezeigt.) Beachten Sie, dass der Benutzer für die erstmalige Anmeldung eine temporäre PIN benötigt.
- **Auffordern des Benutzers zur Eingabe des nächsten Tokens (Next Token-Modus)**
  wenn das vom Benutzer eingegebene Token nicht mit dem von ACE/Server erwarteten Token übereinstimmt. (Der Next Token-Modus ist für Benutzer transparent, die sich über die Seite **RSA SecurID Authentication** anmelden. Die RSA SecurID-Software übergibt das Token über die IVE-Appliance und ohne Benutzerinteraktion an ACE/Server.)

Wenn der Benutzer die neue PIN oder das nächste Token eingibt (je nach Modus), bleiben drei Minuten für die Eingabe der erforderlichen Informationen. Danach bricht das IVE die Transaktion ab und fordert den Benutzer zur erneuten Eingabe der Anmeldeinformationen auf.

Das IVE kann bis zu 200 ACE/Server-Transaktionen gleichzeitig verarbeiten. Eine Transaktion dauert nur so lange wie die Authentifizierung bei ACE/Server. Wenn sich ein Benutzer z. B. am IVE anmeldet, wird die ACE/Server-Transaktion beim Senden der Anforderung durch den Benutzer initiiert. Die Transaktion wird beendet, sobald ACE/Server die Verarbeitung der Anforderung beendet hat. Der Benutzer kann mit der IVE-Sitzung fortfahren, obwohl die ACE/Server-Transaktion beendet wurde.

Das IVE unterstützt die folgenden ACE/Server-Features: New PIN-Modus, Next Token-Modus, DES/SDI-Verschlüsselung, AES-Verschlüsselung, Unterstützung untergeordneter ACE/Server, Namenssperrungen und Clustering. Das IVE unterstützt über das RADIUS-Protokoll auch die New PIN- und Next Token-Modi von RSA SecurID.

Hinweis: Wegen der Einschränkungen der ACE/Server-Bibliothek unter UNIX können Sie u. U. nur eine ACE/Server-Konfiguration festlegen. Informationen zum Erzeugen einer ACE/Agent-Konfigurationsdatei für die IVE-Appliance auf dem ACE-Server finden Sie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 291.

☑ Definieren einer ACE/Serverinstanz

Hinweis: Sie können nur eine ACE/Serverinstanz hinzufügen.

So definieren Sie einen ACE/Server:

1. Erzeugen Sie eine ACE/Agent-Konfigurationsdatei (`sdconf.rec`) für das IVE auf dem ACE-Server (Seite 291).
2. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **ACE Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
4. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.

   Hinweis: Wenn die Endbenutzer SecurID-Softwaretokens an ACE/Server übergeben, können Sie die Verwendung von Leerzeichen oder anderen nicht alphanumerischen Zeichen im Namen der Serverinstanz vermeiden. Um SecurID-Softwaretokenwerte transparent an ACE/Server zu übergeben, müssen Benutzer anhand des folgenden URLs zur Seite „RSA SecurID Authentication" wechseln: **https://IVE/login/ServerInstanz** (wobei „IVE" die IP-Adresse oder den Hostnamen der IVE-Appliance und „ServerInstanz" den oben festgelegten Namen darstellt). Wenn der Name der Serverinstanz Leerzeichen oder andere nicht alphanumerische Zeichen enthält, muss der Benutzer Escapezeichen (z. B. %20) in den URL einfügen.

5. Geben Sie im Feld **ACE Port** einen Standardport an. Das IVE verwendet diese Einstellung nur, wenn in der Datei `sdconf.rec` kein Port angegeben ist.
6. Importieren Sie die RSA ACE/Agent-Konfigurationsdatei. Aktualisieren Sie diese Datei im IVE unbedingt bei jeder Änderung an der Quelldatei. Ebenso müssen Sie, wenn Sie die Instanzdatei aus dem IVE löschen, zur Konfigurationsverwaltungsanwendung für ACE-Server wechseln, wie unter „Generieren einer ACE/Agent-Konfigurationsdatei" auf Seite 291 beschrieben, und das Kontrollkästchen **Sent Node Secret** deaktivieren.
7. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

8. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 379).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 353.

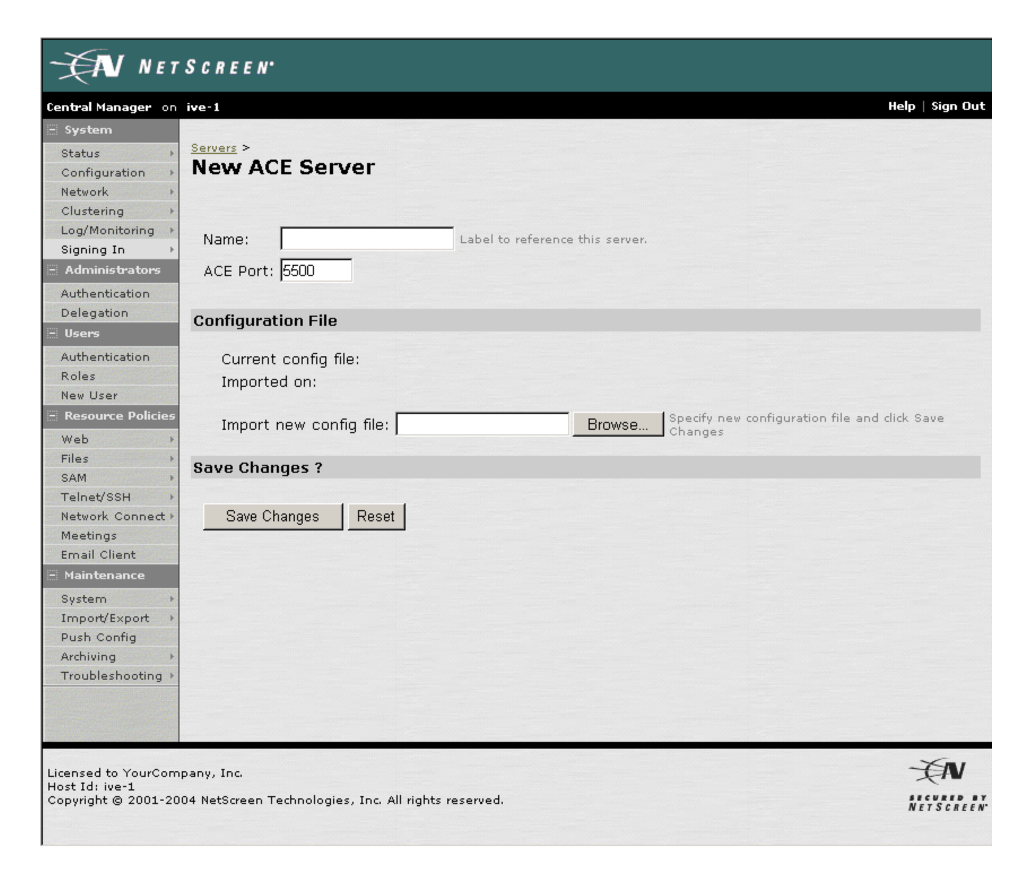


Abbildung 75: **System > Signing In > Servers > ACE Server**

☑ Generieren einer ACE/Agent-Konfigurationsdatei

Wenn Sie ACE/Server für die Authentifizierung verwenden, müssen Sie auf dem ACE-Server eine ACE/Agent-Konfigurationsdatei (`sdconf.rec`) für das IVE generieren.

So generieren Sie eine ACE/Agent-Konfigurationsdatei:

1. Starten Sie die Konfigurationsverwaltungsanwendung für ACE-Server, und klicken Sie auf **Agent Host**.
2. Klicken Sie auf **Add Agent Host**.
3. Geben Sie unter **Name** einen Namen für den IVE-Agenten ein.
4. Geben Sie unter **Network Address** die IP-Adresse des IVE ein.
5. Geben Sie eine auf dem ACE-Server konfigurierte **Site** an.
6. Wählen Sie als **Agent Type** den Typ **Communication Server** aus.
7. Wählen Sie als **Encryption Type** den Typ **DES** aus.
8. Vergewissern Sie sich, dass **Sent Node Secret** (beim Erstellen eines neuen Agenten) deaktiviert ist.

   Wenn der ACE-Server eine vom IVE gesendete Anforderung erfolgreich authentifiziert, wählt der ACE-Server **Sent Node Secret** aus. Wenn der ACE-Server später einen neuen Knotenschlüssel an das IVE senden soll, gehen Sie bei der nächsten Authentifizierungsanforderung folgendermaßen vor:

   1. Deaktivieren Sie das Kontrollkästchen **Sent Node Secret**, indem Sie auf dieses klicken.
   2. Melden Sie sich an der Webkonsole des IVE an, und wählen Sie **System > Signing In > Servers** aus.
   3. Klicken Sie in der Liste **Authentication/Authorization Servers** auf den Namen des entsprechenden ACE-Servers.
   4. Aktivieren Sie unter **Node Verification File** das entsprechende Kontrollkästchen, und klicken Sie auf **Delete**. Durch diese Schritte wird sichergestellt, dass der IVE-Server und der ACE-Server synchronisiert sind. Entsprechend sollten Sie auf dem ACE-Server das Kontrollkästchen **Sent Node Secret** deaktivieren, wenn Sie die Überprüfungsdatei aus dem IVE löschen.
9. Klicken Sie auf **Assign Acting Servers**, und wählen Sie den ACE-Server aus.
10. Klicken Sie auf **Generate Config File**. Wenn Sie den ACE-Server zum IVE hinzufügen, wird diese Konfigurationsdatei importiert.

Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz

Wenn die Benutzerauthentifizierung über einen primären NT-Domänencontroller oder Active Directory erfolgt, melden sich Benutzer am IVE mit dem Benutzernamen und dem Kennwort an, mit denen sie auf den eigenen Windows-Desktop zugreifen. Das IVE unterstützt die Windows NT-Authentifizierung und Active Directory mit Kerberos- oder NTLM-Authentifizierung[1]. Wenn Sie einen systemeigenen Active Directory-Server konfigurieren, können Sie Gruppeninformationen vom Server für die Verwendung in den Rollenzuordnungsregeln eines Bereichs abrufen. In diesem Fall legen Sie den Active Directory-Server als den Authentifizierungsserver des Bereichs fest, und anschließend erstellen Sie eine Rollenzuordnungsregel auf Grundlage der Gruppenmitgliedschaft. Das IVE zeigt alle Gruppen des konfigurierten Domänencontrollers und dessen vertrauenswürdiger Domänen an. Weitere Informationen finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 382.

Hinweis: Das IVE berücksichtigt Vertrauensstellungen in Active Directory und Windows NT-Umgebungen. Benutzer werden nur abgefragt, wenn der Server eine Challenge-Response-Abfrage an das IVE sendet.

☑ Definieren einer Active Directory- oder Windows NT-Domänenserverinstanz

So legen Sie einen Active Directory-Server oder einen Windows NT-Domänenserver fest:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **Active Directory/ Windows NT** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des primären Domänencontrollers oder von Active Directory an.

1. Beim Senden von Benutzeranmeldeinformationen an einen Active Directory-Server wird vom IVE Kerberos verwendet, wenn dies durch den Server unterstützt wird. Andernfalls verwendet das IVE NTLM.

5. Geben Sie die IP-Adresse des Sicherungsdomänencontrollers oder von Active Directory an. (Dies ist optional.)
6. Geben Sie den Domänennamen für die Benutzer ein, denen Sie den Zugriff gewähren möchten. Aktivieren Sie das Kontrollkästchen **Allow domain to be specified as part of username**, um es Benutzern zu ermöglichen, auf der IVE-Anmeldeseite im Feld **Username** einen Domänennamen im folgenden Format einzugeben: Domäne\Benutzername
7. Geben Sie einen Benutzernamen und ein Kennwort für den Administrator ein, damit vom Server folgende Elemente aktiviert werden:
   - Kennwortverwaltung, die für Bereiche verfügbar ist, die für die Authentifizierung einen LDAP- oder Active Directory-Server verwenden. (Diese Option wird auf der Registerkarte **Authentication Policy > Password** des Bereichs aktiviert.)
   - Das Abrufen des Kerberos-Bereichsnamens vom Server durch das IVE (sofern Kerberos vom Server unterstützt wird).

   Hinweis: Nach dem Speichern von Änderungen wird das Kennwort unabhängig von der Kennwortlänge vom IVE mit fünf Sternchen maskiert.

8. Führen Sie unter **Additional Options** folgende Schritte aus:
   - Wenn das IVE den Kerberos-Bereichsnamen anhand der angegebenen Administrator-Anmeldeinformationen vom Active Directory-Server abrufen soll, wählen Sie **Use LDAP to get Kerberos realm name**.
   - Wenn Ihnen der Bereichsname bekannt ist, geben Sie den Kerberos-Bereichsnamen im Feld **Specify Kerberos realm name** ein.
9. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
10. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 379).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 353.

NETSCREEN

Central Manager on ive-1 — Help | Sign Out

System: Status, Configuration, Network, Clustering, Log/Monitoring, Signing In
Administrators: Authentication, Delegation
Users: Authentication, Roles, New User
Resource Policies: Web, Files, SAM, Telnet/SSH, Network Connect, Meetings, Email Client
Maintenance: System, Import/Export, Push Config, Archiving, Troubleshooting

Servers >

New Active Directory / Windows NT

Server

Name: — Label to reference this server
Primary Domain Controller or Active Directory: — Name or IP address
Backup Domain Controller or Active Directory: — Name or IP address
Domain: — NT domain name

☑ Allow domain to be specified as part of username
☐ Allow trusted domains

Administrator

Admin Username: — Required for Password Management
Admin Password:

Additional Options

◉ Use LDAP to get Kerberos realm name
○ Specify Kerberos realm name

Save Changes | Reset

Licensed to YourCompany, Inc.
Host Id: ive-1

SECURED BY NETSCREEN

Abbildung 76: **System > Signing In > Servers > Active Directory/Windows NT**

Konfigurieren einer Instanz eines anonymen Servers

Ein anonymer Server ermöglicht Benutzern den Zugriff auf das IVE ohne Angabe von Benutzername oder Kennwort. Wenn ein Benutzer den URL einer Anmeldeseite eingibt, für die Authentifizierung durch einen anonymen Server konfiguriert ist, umgeht das IVE die IVE-Standardanmeldeseite und zeigt dem Benutzer sofort die IVE-Willkommensseite an.

Sie können anonyme Authentifizierung auswählen, wenn Sie es nicht für notwendig halten, dass die Ressourcen auf dem IVE sehr hohen Sicherheitsanforderungen unterliegen oder wenn Sie die anderen Sicherheitsmaßnahmen auf dem IVE für ausreichend halten. Sie können z. B. eine Benutzerrolle mit beschränktem Zugriff auf interne Ressourcen erstellen und diese Rolle dann mithilfe einer Richtlinie authentifizieren, die nur verlangt, dass sich Benutzer von einer IP-Adresse aus Ihrem internen Netzwerk anmelden. Bei dieser Methode wird davon ausgegangen, dass ein Benutzer, der zum Zugriff auf das interne Netzwerk berechtigt ist, auch die Ressourcen anzeigen darf, die im Rahmen dieser Benutzerrolle bereitgestellt werden.

Beachten Sie bei der Definition und Überwachung einer Instanz eines anonymen Servers Folgendes:

- Sie können nur eine Konfiguration für anonyme Server hinzufügen.
- Administratoren können nicht mithilfe eines anonymen Servers authentifiziert werden.
- Bei der Konfiguration müssen Sie auf der Registerkarte **Users > Authentication > General** den anonymen Server als Authentifizierungs-server und als Verzeichnis-/Attributserver auswählen (Seite 379).
- Beim Erstellen von Rollenzuordnungsregeln auf der Registerkarte **Users > Authentication > Role Mapping** (Seite 382) gestattet das IVE keine Erstellung von Zuordnungsregeln, die für bestimmte Benutzer gelten (z. B. „Joe“), da auf einem anonymen Server keine Informationen zu Benutzernamen gespeichert werden. Sie können Rollenzuordnungs-regeln erstellen, die auf einem Standardbenutzernamen (*), Zertifikat-attributen oder benutzerdefinierten Ausdrücken basieren.
- Aus Sicherheitsgründen können Sie ggf. die Anzahl der Benutzer beschränken, die sich gleichzeitig über einen anonymen Server anmelden. Verwenden Sie dazu die Option auf der Registerkarte **Users > Authentication > [Bereich] > Authentication Policy > Limits**. Dabei ist **[Bereich]** der Bereich, für Benutzerauthentifizierung durch den anonymen Server konfiguriert ist (Seite 381).

- Sie können die Sitzungen von anonymen Benutzern (im Gegensatz zu anderen Authentifizierungsservern) nicht löschen und nicht über die Registerkarte **Users** anzeigen, da keine Benutzernamen eingegeben wurden und das IVE daher keine individuellen Sitzungsdaten anzeigen kann.

☑ Definieren einer Instanz eines anonymen Servers

So definieren Sie einen anonymen Server:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **Anonymous Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Klicken Sie auf **Save Changes**.
5. Geben Sie die Bereiche an, die der Server für die Autorisierung von Benutzern verwenden soll (Seite 379).

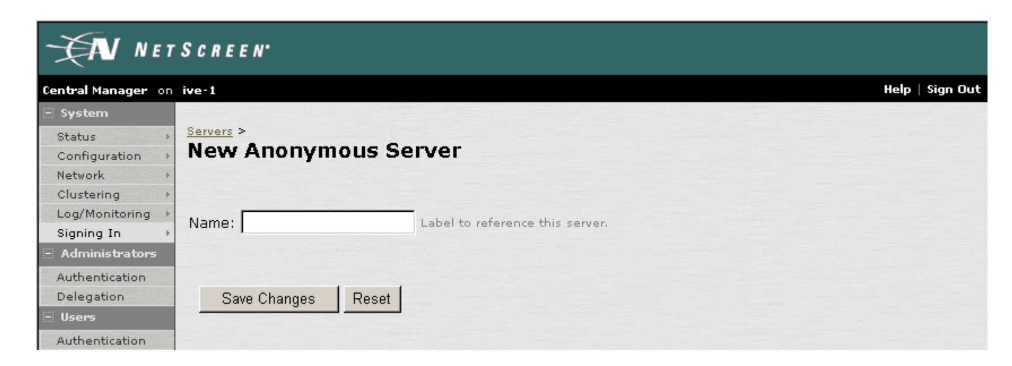


Abbildung 77: **System > Signing In > Servers > Anonymous Server**

Konfigurieren einer Zertifikatserverinstanz

Der Zertifikatserver ermöglicht die Authentifizierung von Benutzern anhand von Attributen in clientseitigen Zertifikaten. Sie können den Zertifikatserver allein oder in Verbindung mit einem anderen Server verwenden, um Benutzer zu authentifizieren und sie Rollen zuzuordnen.

Sie könnten Benutzer z. B. allein anhand ihrer Zertifikatattribute authentifizieren. Wenn das IVE ermittelt, dass das Benutzerzertifikat gültig ist, wird der Benutzer anhand der von Ihnen festgelegten Zertifikatattribute angemeldet, ohne aufgefordert zu werden, einen Benutzernamen oder ein Kennwort einzugeben.

Sie können Benutzer auch authentifizieren, indem Sie ihre Clientzertifikatattribute an einen zweiten Authentifizierungsserver (wie LDAP) weiterleiten. In diesem Szenario ermittelt der Zertifikatserver zunächst, ob das Benutzerzertifikat gültig ist. Anschließend kann das IVE Zuordnungsregeln der Bereichsebene verwenden, um die Zertifikatattribute mit den LDAP-Attributen des Benutzers zu vergleichen. Wenn keine entsprechende Übereinstimmung gefunden wird, kann der Benutzerzugriff entsprechend Ihren Angaben vom IVE verweigert oder eingeschränkt werden.

Wichtig: Bei Verwendung clientseitiger Zertifikate wird dringend empfohlen, die Endbenutzer anzuweisen, ihren Webbrowser nach dem Abmelden vom IVE zu schließen. Andernfalls können andere Benutzer über deren geöffnete Browsersitzungen auf durch Zertifikate geschützte Ressourcen auf dem IVE ohne erneute Authentifizierung zugreifen. (Nach dem Laden eines clientseitigen Zertifikats werden die im Zertifikat gespeicherten Anmeldinformationen und der private Schlüssel von Internet Explorer und Netscape zwischengespeichert. Diese Informationen bleiben in den Browsern zwischengespeichert, bis der Browser vom Benutzer geschlossen wird (in manchen Fällen, bis die Arbeitsstation neu gestartet wird). Ausführliche Informationen finden Sie unter: http://support.microsoft.com/?kbid=290345. Sie können die Benutzer daran erinnern, ihren Browser zu schließen, indem Sie die Meldung für die Abmeldung auf der Registerkarte **System > Signing In > Sign-in Pages** ändern.

☑ Festlegen einer Zertifikatserverkonfiguration

Gehen Sie zum Festlegen eines Zertifikatservers auf dem IVE folgendermaßen vor:

1. Verwenden Sie die Einstellungen auf der Registerkarte **System > Configuration > Certificates > CA Certificates**, um das zum Signieren der clientseitigen Zertifikate verwendete Zertifikat der Zertifizierungsstelle zu importieren.

2. Konfigurieren Sie eine Zertifikatserverinstanz:
    1. Navigieren Sie zu **System > Signing In > Servers**.
    2. Wählen Sie aus der Liste **New** den Eintrag **Certificate Server** aus, und klicken Sie anschließend auf **New Server**.
    3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
    4. Geben Sie im Feld **User Name Template** an, wie das IVE einen Benutzernamen erstellen soll. Sie können jede beliebige Kombination von Zertifikatsvariablen in spitzen Klammern und Klartext verwenden. Eine Liste von Zertifikatsvariablen finden Sie unter „Systemvariablen und Beispiele“ auf Seite 601.

        Hinweis: Wenn Sie ein Zertifikatattribut mit mehr als einem Wert auswählen, verwendet das IVE den ersten übereinstimmenden Wert. Wenn Sie z. B. `<certDN.OU>` eingeben und dem Benutzer zwei Werte für das Attribut vorliegen (`ou=management`, `ou=sales`), verwendet das IVE den Wert „`management`“. Wenn alle Werte verwendet werden sollen, fügen Sie der Variable das Attribut `SEP` hinzu. Wenn Sie z. B. `<certDN.OU SEP=„:“>` eingeben, verwendet das IVE „management:sales“.

    5. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

        Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 353.

3. Wenn Zertifikatattribute mithilfe eines LDAP-Servers überprüft werden sollen, erstellen Sie anhand der Einstellungen auf der Seite **System > Signing In > Servers** eine LDAP-Serverinstanz. Beachten Sie, dass Sie zum Abrufen der benutzerspezifischen Attribute, die über das Zertifikat überprüft werden sollen, den Abschnitt **Finding user entries** auf der LDAP-Konfigurationsseite verwenden müssen.
4. Legen Sie anhand der Einstellungen auf den Registerkarten **Users > Authentication > Authentication > General** bzw. **Administrators > Authentication > General** fest, welche Bereiche den Zertifikatserver zum Authentifizieren von Benutzern verwenden sollen. (Anhand der Einstellungen dieser Registerkarten können Sie auch Bereiche angeben, die einen LDAP-Server zum Überprüfen von Zertifikatattributen verwenden sollen.)
5. Ordnen Sie anhand der Einstellungen auf der Seite **System > Signing In > Sign-in Policies** die im vorherigen Schritt konfigurierten Bereiche einzelnen Anmelde-URLs zu.

6. Wenn der Benutzerzugriff auf Bereiche, Rollen oder Ressourcenrichtlinien auf Grundlage einzelner Zertifikatattribute eingeschränkt werden soll, verwenden Sie die unter „Zertifikateinschränkungen" auf Seite 587 beschriebenen Einstellungen.

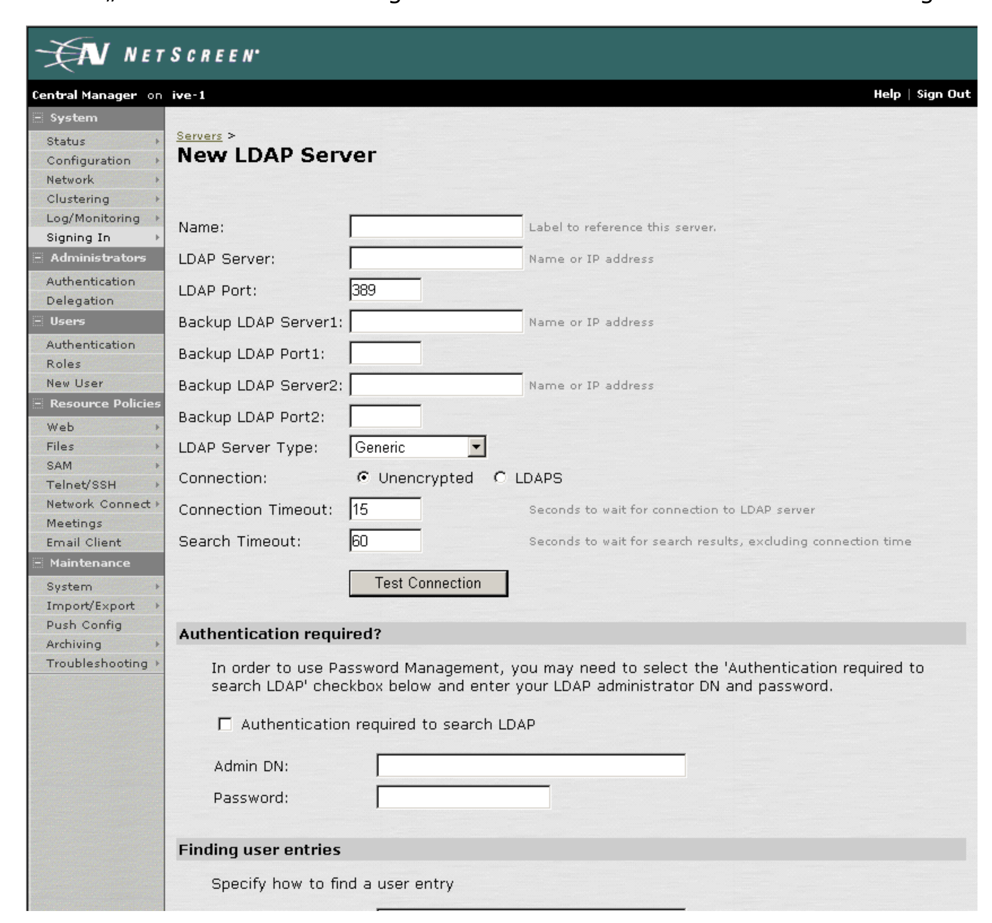


Abbildung 78: System > Signing In > Servers > Certificate Server

Konfigurieren einer LDAP-Serverinstanz

Das IVE unterstützt zwei LDAP-spezifische Authentifizierungsoptionen:

- **Unencrypted** – Das IVE sendet den Benutzernamen und das Kennwort in einfachem Klartext an den LDAP-Verzeichnisdienst.
- **LDAPS** – Das IVE verschlüsselt die Daten in der LDAP-Authentifizierungssitzung mit dem SSL-Protokoll (Secure Socket Layer), bevor sie an den LDAP-Verzeichnisdienst gesendet werden.

Das IVE unterstützt außerdem dynamische LDAP-Gruppen und LDAP-Kennwortverwaltung über das IVE. Mithilfe der Kennwortverwaltung können Benutzer, die sich über einen LDAP-Server authentifizieren, ihre Kennwörter anhand der auf dem LDAP-Server definierten Richtlinien über das IVE zu verwalten[1]. Beispiel: Ein Benutzer verwendet für die Anmeldung am IVE ein Kennwort, dessen Gültigkeit in Kürze abläuft. Das IVE fängt die Benachrichtigung über das abgelaufene Kennwort ab, zeigt sie dem Benutzer in der IVE-Oberfläche an und leitet dann die Antwort des Benutzers an den LDAP-Server zurück, ohne dass sich der Benutzer separat am LDAP-Server anmelden muss.

Weitere Informationen finden Sie unter:

☑ Definieren einer LDAP-Serverinstanz

So definieren Sie eine LDAP-Serverinstanz:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Zum Erstellen einer neuen Serverinstanz auf dem IVE wählen Sie aus der Liste **New** den Eintrag **LDAP Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des LDAP-Servers an, der vom IVE zur Überprüfung von Benutzern verwendet wird.

1. Die LDAP-Kennwortverwaltung ist eine lizenzierte Funktion.

5. Geben Sie den Port an, den der LDAP-Server überwacht. Dies ist bei Verwendung einer unverschlüsselten Verbindung normalerweise Port 389 und bei Verwendung von SSL Port 636.
6. Geben Sie Parameter für LDAP-Sicherungsserver an (optional). Das IVE verwendet die angegebenen Server für die Failover-Verarbeitung. Jede Authentifizierungsanforderung wird zuerst an den primären LDAP-Server und dann an den oder die angegebenen Sicherungsserver weitergeleitet, falls der primäre Server nicht erreichbar ist.

Hinweis: LDAP-Sicherungsserver müssen dieselbe Version wie der primäre LDAP-Server aufweisen. Darüber hinaus empfiehlt es sich, nicht den Hostnamen, sondern die IP-Adresse eines LDAP-Sicherungsservers anzugeben, denn dadurch kann die Failover-Verarbeitung beschleunigt werden, da der Hostname nicht in eine IP-Adresse aufgelöst werden muss.

7. Geben Sie an, ob die Verbindung zwischen dem IVE und dem LDAP-Verzeichnisdienst unverschlüsselt bleiben oder ob SSL (LDAPs) verwendet werden soll.
8. Geben Sie den Typ des LDAP-Servers an, über den Sie Benutzer authentifizieren möchten.
9. Klicken Sie auf **Test Connection**, um die Verbindung zwischen der IVE-Appliance und den angegebenen LDAP-Servern zu prüfen. (Dies ist optional.)
10. Aktivieren Sie das Kontrollkästchen **Authentication required to search LDAP**, wenn das IVE über das LDAP-Verzeichnis authentifiziert werden soll, um eine Suche durchzuführen oder Kennwörter mithilfe der Kennwortverwaltungsfunktion zu ändern (Seite 306). Geben Sie anschließend einen Administrator-DN und ein Kennwort ein.

    Beispiel-DN: `CN=Administrator,CN=Users,DC=eng,DC=Juniper,DC=com`
11. Geben Sie unter **Finding user entries** Folgendes an:
    - **Base DN**, von dem an nach Benutzereinträgen gesucht werden soll.

      Beispiel: `DC=eng,DC=Juniper,DC=com`
    - **Filter**, wenn die Suche eingegrenzt werden soll.

      Beispiel: `samAccountname=<USER>` oder `cn=<USER>`
      - Fügen Sie zur Verwendung des Benutzernamens, der auf der Anmeldeseite für die Suche eingegeben wurde, im Filter die Zeichenfolge `<USER>` (in Großbuchstaben) ein.
      - Geben Sie einen Filter an, der keinen (0) oder einen (1) Benutzer-DN pro Benutzer zurückgibt. Falls mehrere DNs zurückgegeben werden, verwendet das IVE den ersten zurückgegebenen DN.

12. Das IVE unterstützt sowohl statische als auch dynamische Gruppen. Zum Aktivieren des Gruppenlookups müssen Sie angeben, wie das IVE den LDAP-Server nach einer Gruppe durchsuchen soll. Geben Sie unter **Determining group membership** Folgendes an:
    - **Base DN**, ab dem die Suche nach Benutzergruppen beginnen soll.
    - **Filter**, wenn die Suche nach einer Benutzergruppe optimiert werden soll.
    - **Member Attribute**, um alle Mitglieder einer statischen Gruppe zu identifizieren.

      Active Directory-Beispiel: `member`

      iPlanet-Beispiel: `uniquemember`
    - **Query Attribute**, um eine LDAP-Abfrage anzugeben, die die Mitglieder einer dynamischen Gruppe zurückgibt.

      iPlanet-Beispiel: `memberURL`
    - **Nested Group Level**, um anzugeben, wie viele Ebenen innerhalb einer Gruppe nach dem Benutzer durchsucht werden sollen. Beachten Sie Folgendes: Je höher die Anzahl, desto länger die Abfragezeit. Daher wird empfohlen, für die Suche nicht mehr als zwei Ebenen anzugeben.
13. Wählen Sie unter **Bind Options** Folgendes aus:
    - **Simple bind**, um die Anmeldeinformationen eines Benutzers im Klartext (unverschlüsselt) an den LDAP-Verzeichnisdienst zu senden.
    - **StartTLS bind**, um die Anmeldeinformationen eines Benutzers über das TLS-Protokoll (Transport Layer Security) zu verschlüsseln, bevor das IVE die Daten an den LDAP-Verzeichnisdienst sendet.
14. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
15. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 379).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 353.

Unterstützte Funktionen für die LDAP-Kennwortverwaltung

In diesem Abschnitt werden die LDAP-Kennwortrichtlinien sowie die Sperrungs- und Validierungsfunktionen beschrieben, die das IVE bei der Authentifizierung mit Microsoft Active Directory-, Sun iPlanet- und Novell eDirectory-LDAP-Servern unterstützt. Diese Funktionen müssen durch den LDAP-Server selbst festgelegt werden, bevor das IVE die entsprechenden Meldungen, Funktionen und Beschränkungen an Endbenutzer weitergeben kann. Bei der Authentifizierung mit einem generischen LDAP-Server wie IBM Secure Directory unterstützt das IVE nur die Authentifizierung und erlaubt es Benutzern, ihre Kennwörter zu ändern. Beachten Sie beim Verwenden von Active Directory Folgendes:

- Das Aktualisieren einer Richtlinie kann in Active Directory bis zu 90 Minuten dauern. Die alten Richtlinieneinstellungen bleiben in Kraft, bis Active Directory die Aktualisierung einer Richtlinie vollständig abgeschlossen hat.
- Damit das Ändern von Kennwörtern beim Verwenden der Active Directory-Kennwortverwaltung unterstützt wird, müssen Sie LDAPS auf dem Active Directory-Server aktivieren, z. B. durch Importieren eines gültigen signierten SSL-Zertifikats in den Speicher für persönliche Zertifikate (Personal Certificates Store) (bei Verwendung der MMC und bei Auswahl des Zertifikats-Snap-Ins verfügbar). Das CN Subject dieses Zertifikats muss genau mit dem Hostnamen des Active Directory-Servers übereinstimmen. Das SSL-Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle signiert sein. Dies kann auch lokale Zertifizierungsstellen einschließen, sofern diese als vertrauenswürdig gelten. Beachten Sie, dass das Stammzertifikat im Stammzertifikatspeicher (Root Certificates Store) installiert sein muss, damit eine Vertrauensstellung hergestellt werden kann.

Unterstützte Funktionen für Kennwortrichtlinien:

- Authentifizieren des IVE-Benutzers durch den LDAP-Server.
- Dem Benutzer gestatten, sein LDAP-Kennwort auf der IVE-Seite **System > Preferences** zu ändern.
- Abmelden des Benutzers vom IVE nach erfolgreicher Änderung des LDAP-Kennwortes.

- Festlegen, dass der Benutzer sein LDAP-Kennwort bei der nächsten Anmeldung am IVE ändern muss.

Hinweis: Wenn Sie diese Option für einen iPlanet-Server aktivieren, müssen Sie beachten, dass Sie sich anschließend am Directory Manager anmelden und das Kennwort des Benutzers ändern müssen, um den Benutzer zurückzusetzen. Bei der nächsten Anmeldung des Benutzers mit dem neuen Kennwort, wird der Benutzer vom IVE zum Ändern seines Kennwortes aufgefordert.

- Benachrichtigen des Benutzers über den Ablauf des LDAP-Kennwortes.
- Den Benutzer 14 Tage im Voraus vom Ablauf seines LDAP-Kennwortes informieren.

Hinweis: Beim Aktivieren dieser Option auf einem der folgenden Server:
– iPlanet-Server. Beachten Sie, dass das IVE nur Richtlinien für das Ablaufen von Kennwörtern auf Benutzerebene erkennt, keine Richtlinien auf Gruppenebene.
– Active Directory-Server. Beachten Sie, dass das Kontoablaufdatum keinen Einfluss auf das Ablaufdatum des Benutzerkennwortes hat.

Unterstützte Funktionen für die Kennwortsperrung:

- Sperren des Zugriffs auf das IVE und den LDAP-Server, wenn das Kennwort des Benutzers deaktiviert oder gesperrt ist.

Unterstützte Funktionen für die Kennwortvalidierung:

- Erzwingen einer Mindestlänge für LDAP-Kennwörter.
- Erzwingen eines Mindestalters für LDAP-Kennwörter, um zu verhindern, dass der Benutzer sein Kennwort zu häufig ändert.
- Festlegen einer Komplexitätsanforderung für LDAP-Kennwörter, um zu verhindern, dass der Benutzer seinen Benutzernamen, seinen Vornamen oder seinen Nachnamen im Kennwort verwendet. Außerdem soll das Kennwort 3 Zeichen aus den folgenden Kategorien enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (beispielsweise !, $, %).
- Berücksichtigen der LDAP-Kennworthistorie des Benutzers.

Wenn Sie den Wert für die Kennworthistorie auf null festlegen, kann der Benutzer dasselbe Kennwort sofort erneut verwenden.

NETSCREEN

Central Manager on ive-1 — Help | Sign Out

System: Status, Configuration, Network, Clustering, Log/Monitoring, Signing In
Administrators: Authentication, Delegation
Users: Authentication, Roles, New User
Resource Policies: Web, Files, SAM, Telnet/SSH, Network Connect, Meetings, Email Client
Maintenance: System, Import/Export, Push Config, Archiving, Troubleshooting

Servers >

New LDAP Server

Name: ______ Label to reference this server.
LDAP Server: ______ Name or IP address
LDAP Port: 389
Backup LDAP Server1: ______ Name or IP address
Backup LDAP Port1: ______
Backup LDAP Server2: ______ Name or IP address
Backup LDAP Port2: ______
LDAP Server Type: Generic
Connection: (•) Unencrypted ( ) LDAPS
Connection Timeout: 15 Seconds to wait for connection to LDAP server
Search Timeout: 60 Seconds to wait for search results, excluding connection time

[Test Connection]

Authentication required?

In order to use Password Management, you may need to select the 'Authentication required to search LDAP' checkbox below and enter your LDAP administrator DN and password.

☐ Authentication required to search LDAP

Admin DN: ______
Password: ______

Finding user entries

Specify how to find a user entry

Base DN: ______ example: dc=sales,dc=com
Filter: ______ example: cn=<USER>

Determining group membership

If group membership is NOT reflected as attributes of a user's entry, specify how to find a group entries. Note that these are default settings that you can override on a per-group basis in the Server Catalog.

Base DN: ______ example: dc=sales,dc=com
Filter: ______ example: cn=<GROUPNAME>
Member Attribute: ______ Attribute used to identify members of a static group
Query Attribute: ______ Attribute used to determine members of a dynamic group
Nested Group Level: ______ Maximum depth of nested group

Bind options

If this server will be used to authenticate users, select one of the following methods for binding.

Bind method: ( ) Simple bind
(•) StartTLS bind

Abbildung 79: System > Signing In > Servers > LDAP Server

Konfigurieren einer lokalen IVE-Server-Instanz

Im IVE können Sie eine oder mehrere lokale Datenbanken für vom IVE authentifizierte Benutzer erstellen. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie eine Gruppe von temporären Benutzern erstellen möchten. Hinweis: Alle Administratorenkonten werden als lokale Datensätze gespeichert, Administratoren können jedoch über einen externen Server authentifiziert werden. Anweisungen hierfür finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich" auf Seite 381.

In diesem Abschnitt werden folgende Vorgänge behandelt:

☑ Definieren einer lokalen IVE-Server-Instanz

So definieren Sie einen lokalen IVE-Server:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **IVE Authentication** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Users** und **Admin Users** angezeigt.
5. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 379).

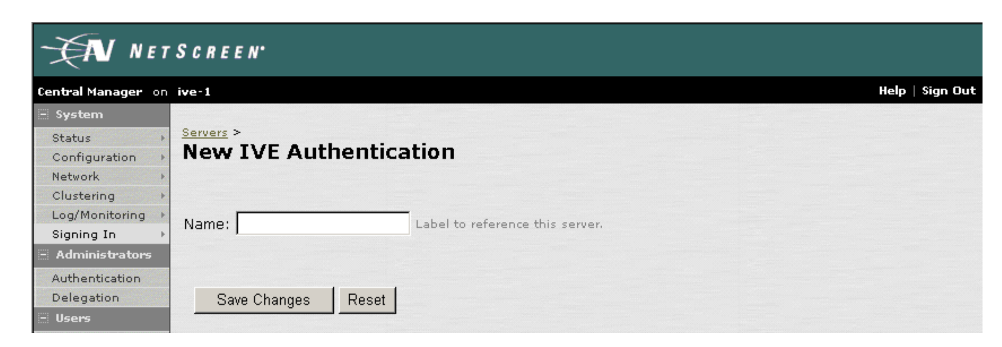


Abbildung 80: **System > Signing In > Servers > Local IVE Authentication**

☑ Erstellen lokaler Benutzer

Wenn Sie als Typ des Authentifizierungsservers „IVE Authentication" auswählen, müssen Sie für diese Datenbank Datensätze für lokale Benutzer definieren. Lokale Benutzerdatensätze bestehen aus einem Benutzernamen, dem vollständigen Namen und dem Kennwort des Benutzers. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie schnell eine Gruppe von temporären Benutzern erstellen möchten.

So erstellen Sie lokale Benutzerdatensätze für die lokale IVE-Authentifizierung:

1. Führen Sie in der Webkonsole einen der folgenden Vorgänge aus:
   - Wählen Sie **System > Signing In > Servers** aus, und klicken Sie auf die IVE-Datenbank, der Sie ein Benutzerkonto hinzufügen möchten. Klicken Sie auf die Registerkarte **Users** und dann auf **New**.
   - Wählen Sie **Users > New User** aus.
2. Geben Sie den Benutzernamen, den vollständigen Namen des Benutzers und ein Kennwort ein. Hinweis:
   - In Benutzernamen darf die Zeichenkombination „~~" nicht enthalten sein.
   - Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto erstellen.
3. (Nur auf der Seite **Users > New User**) Wählen Sie aus der Liste **Authenticate Using** die IVE-Datenbank aus, der Sie ein Benutzerkonto hinzufügen möchten.
4. Klicken Sie auf **Save Changes**. Der Benutzerdatensatz wird der IVE-Datenbank hinzugefügt.

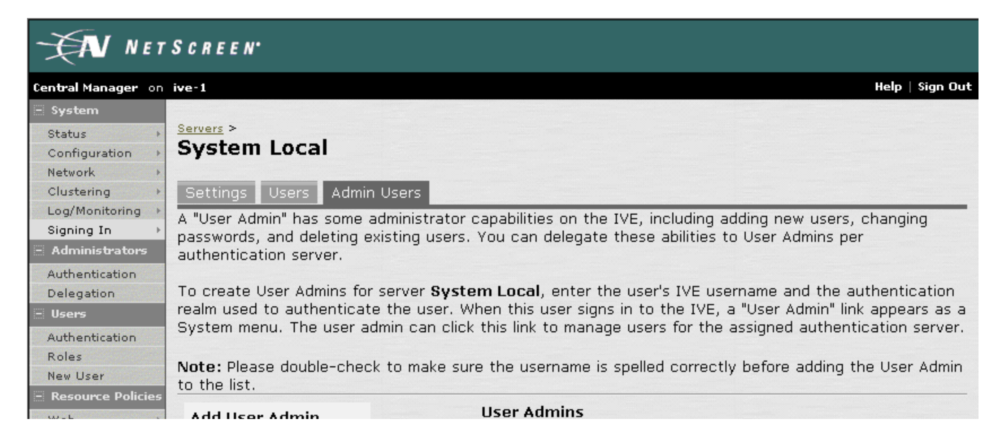


Abbildung 81: **Users > Signing In > Servers > Local IVE Authentication > Users > New User**

☑ Verwalten von Benutzerkonten

Die Konfigurationsseite für lokale IVE-Authentifizierungsserver enthält eine Registerkarte **Users**, auf der Sie aktive IVE-Benutzerkonten anzeigen, bearbeiten und löschen können.

So verwalten Sie ein lokales Benutzerkonto:

1. Wählen Sie in der Webkonsole **System > Signing In > Servers** aus.
2. Klicken Sie in der Liste **Authentication/Authorization Servers** auf die entsprechende Verknüpfung.
3. Klicken Sie auf die Registerkarte **Users**.
4. Führen Sie eine der folgenden Aufgaben durch:
   - Geben Sie im Feld **Show Users Named** einen Benutzernamen ein, und klicken Sie auf **Update**, um nach einem bestimmten Benutzer zu suchen.

     Sie können auch ein Sternchen (`*`) als Platzhalter verwenden, das für eine beliebige Anzahl von Zeichen steht (null, eins oder mehrere). Wenn Sie z. B. nach allen Benutzernamen suchen möchten, die die Buchstaben `jo` enthalten, geben Sie im Feld **Show users named** die Zeichenfolge `*jo*` ein. Bei der Suche wird die Groß- und Kleinschreibung berücksichtigt. Wenn Sie wieder die Gesamtliste der Gruppenkonten anzeigen möchten, geben Sie ein Sternchen (`*`) ein, oder löschen Sie den Feldinhalt, und klicken Sie dann auf **Update**.

- Geben Sie im Feld **Show N users** eine Zahl ein, und klicken Sie auf **Update**, um die Anzahl von Benutzern anzugeben, die auf der Seite angezeigt werden.
- Aktivieren Sie das Kontrollkästchen neben den jeweiligen Benutzern, und klicken Sie anschließend auf **Delete**, um deren IVE-Sitzungen zu beenden.

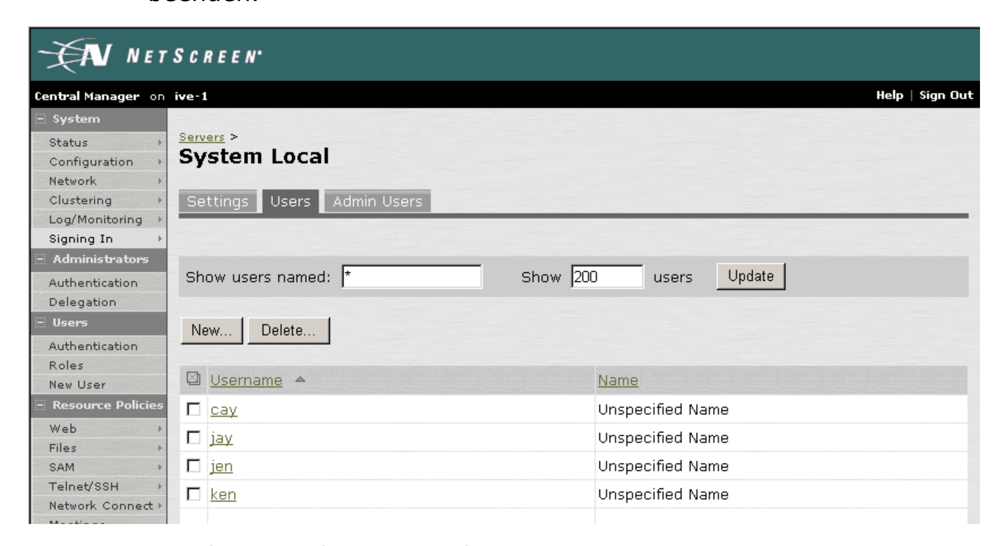


Abbildung 82: **System > Signing In > Servers > Local IVE Authentication > Users**

☑ Delegieren von Benutzerverwaltungsrechten an Endbenutzer

Auf der Registerkarte **System > Signing In > Admin Users** können Sie Benutzerverwaltungsrechte an ausgewählte Endbenutzer delegieren, einschließlich des Rechts, Benutzer zu einem lokalen IVE-Authentifizierungsserver hinzuzufügen, Benutzer zu löschen, vollständige Namen von Benutzern zu bearbeiten und Benutzerkennwörter über das Menü **User Admin** auf der Startseite des sicheren Gateways zu ändern.

Hinweis: Benutzeradministratoren können nur lokale IVE-Authentifizierungsserver verwalten. Außerdem dürfen Benutzeradministratoren keine Bereiche oder Rollenzuordnungen verwalten. Daher wird die Aktivierung der Funktion „User Admin“ nur dann empfohlen, wenn die Rollenzuordnungsregeln des Authentifizierungsbereichs es nicht zugeordneten Benutzern (*) erlauben, sich am IVE anzumelden, sodass der Benutzeradministrator neue Benutzer ohne Eingreifen des Administrators hinzufügen kann. (Wenn die Rollenzuordnungen automatisch erfolgen, können Benutzeradministratoren die neuen Benutzer ohne Hilfe des Administrators manuell einer Rolle zuordnen.)

So delegieren Sie Benutzerverwaltungsrechte an einen Endbenutzer:

1. Wählen Sie in der Webkonsole **System > Signing In > Servers** aus.
2. Wählen Sie die lokale IVE-Authentifizierungsserver-Instanz aus, die vom Benutzeradministrator verwaltet werden soll, und klicken Sie dann auf die Registerkarte **Admin Users**.

   Hinweis: Benutzeradministratoren können nur lokale IVE-Authentifizierungsserver verwalten.

3. Geben Sie den **Username** des Benutzers ein, der Konten für den ausgewählten Authentifizierungsserver verwalten soll. (Der ausgewählte Benutzer muss auf dem Server, den er verwaltet, nicht als lokaler Benutzer hinzugefügt werden.)

   Hinweis: Achten Sie bei der Eingabe des Benutzernamens des Benutzeradministrators auf die exakte Zeichenfolge. Diese muss genau übereinstimmen.

4. Wählen Sie den **Authentication Realm** aus, dem der Benutzeradministrator zugeordnet wird, wenn er sich am IVE anmeldet.
5. Klicken Sie auf **Add**. Das IVE fügt den neuen Benutzeradministrator der Liste **User Admins** im folgenden Format hinzu: `Benutzername@Servername`.
6. Wenn der angegebene Benutzeradministrator mehreren Bereichen zugeordnet ist, wiederholen Sie ggf. die Schritte 3 bis 5, sodass der Benutzer den Server unabhängig von dem Konto verwalten kann, über das er sich beim IVE anmeldet.
7. Um dem Benutzer die Verwaltungsrechte wieder zu entziehen, wählen Sie in der Liste **User Admins** den entsprechenden Namen aus, und klicken Sie auf **Remove**.

Hinweis: Informationen zum Verwalten von Benutzern über die Startseite des sicheren Gateways finden Sie in der Hilfe zum sicheren Gateway im Thema „Hinzufügen, Ändern und Löschen von Benutzern“, d. h. in der über das IVE verfügbaren Benutzerhilfe.

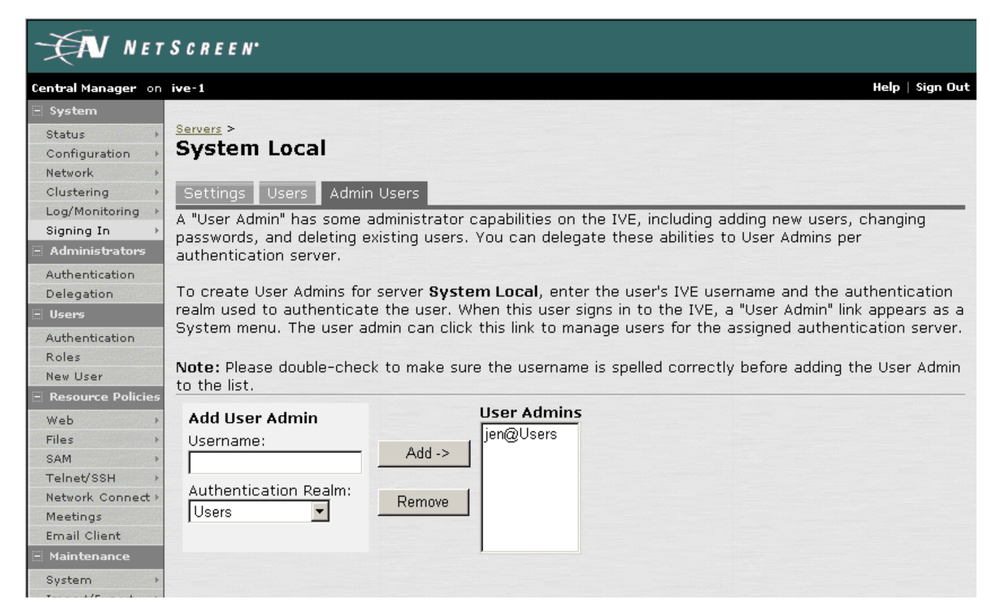


Abbildung 83: **System > Signing In > Servers > Local IVE Authentication > Users**

Konfigurieren einer NIS-Serverinstanz

Beim Authentifizieren von Benutzern mit einem UNIX/NIS-Server überprüft der IVE, ob der auf der Anmeldeseite eingegebene Benutzername und das Kennwort einem gültigen Paar aus Benutzer-ID und Kennwort auf dem NIS-Server entsprechen. Beachten Sie, dass der an das IVE gesendete Benutzername keine zwei aufeinander folgenden Tilden (~~) enthalten darf.

Hinweis: Sie können NIS-Authentifizierung nur mit dem IVE verwenden, wenn die Kennwörter auf dem NIS-Server im Crypt- oder MD5-Format gespeichert sind. Außerdem können Sie dem IVE nur eine NIS-Serverkonfiguration hinzufügen, mit der jedoch eine beliebige Anzahl von Bereichen authentifiziert werden können.

☑ Festlegen einer NIS-Serverinstanz

So definieren Sie eine NIS-Serverinstanz:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **NIS Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des NIS-Servers an.
5. Geben Sie den Domänennamen für den NIS-Server an.
6. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
7. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 379).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 353.

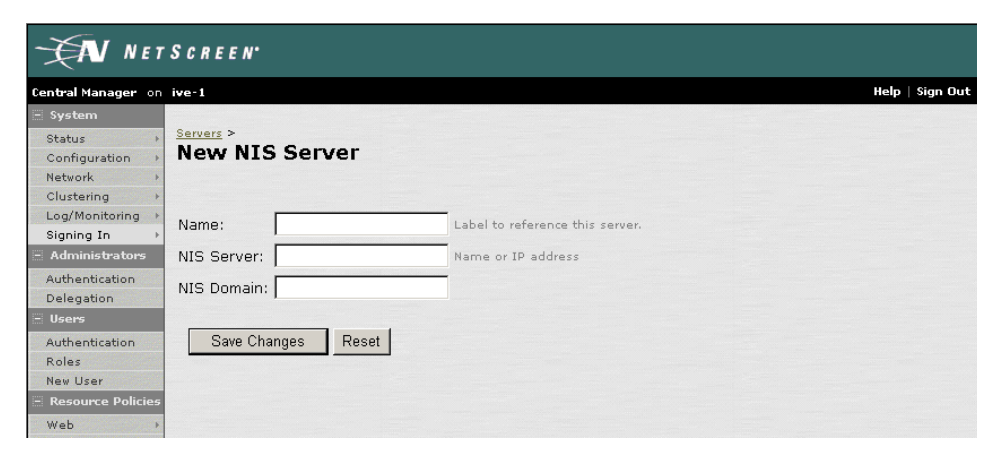


Abbildung 84: System > Signing In > Servers > NIS Server

Konfigurieren einer RADIUS-Serverinstanz

Beim Authentifizieren von Benutzern mit einem RADIUS-Server müssen Sie den RADIUS-Server so konfigurieren, dass der IVE als Client erkannt wird. Außerdem müssen Sie für den RADIUS-Server einen gemeinsamen geheimen Schlüssel zur Verwendung bei der Authentifizierung der Clientanforderung angeben.

Der IVE unterstützt die RADIUS-Standardauthentifizierungsschemas. Zu diesen gehören folgende: Access-Request, Access-Accept, Access-Reject und Access-Challenge. Der IVE unterstützt auch RSA ACE/Server unter Verwendung des RADIUS-Protokolls und eines SecurID-Tokens (erhältlich von Security Dynamics). Wenn Sie für die Authentifizierung von Benutzern SecurID verwenden, müssen die Benutzer ihre Benutzer-ID und die Kombination aus PIN und dem Tokenwert angeben.

Wenn Sie einen PassGo Defender-RADIUS-Server verwenden, erfolgt die Benutzeranmeldung folgendermaßen:

1. Der Benutzer meldet sich beim IVE mit einem Benutzernamen und einem Kennwort an. Das IVE leitet diese Anmeldeinformationen an Defender weiter.
2. Defender sendet eine eindeutige Anfragezeichenfolge an das IVE, und im IVE wird diese Anfragezeichenfolge dem Benutzer angezeigt.
3. Der Benutzer gibt die Anfragezeichenfolge in einem Defender-Token ein, und das Token erzeugt eine Antwortzeichenfolge.
4. Der Benutzer gibt die Antwortzeichenfolge im IVE ein und klickt auf **Sign In**.

☑ Definieren eines RADIUS-Servers

So legen Sie einen RADIUS-Server fest:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie in der Liste **New** den Eintrag **Radius Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.

4. Geben Sie den Namen oder die IP-Adresse des RADIUS-Servers an.
5. Geben Sie die Portangabe für den RADIUS-Server ein. Normalerweise ist dies Port 1645.
6. Geben Sie eine Zeichenfolge für den gemeinsamen geheimen Schlüssel ein. Sie müssen diese Zeichenfolge auch eingeben, wenn Sie den RADIUS-Server für die Erkennung des IVE-Geräts als Client konfigurieren.
7. Geben Sie die Zeitspanne ein, für die das IVE auf eine Antwort vom RADIUS-Server bis zur Zeitüberschreitung für die Verbindung warten soll.
8. Geben Sie die Anzahl der weiteren Verbindungsversuche ein, die das IVE nach dem ersten fehlgeschlagenen Versuch ausführen soll.
9. Geben Sie einen sekundären RADIUS-Server an, der vom IVE verwendet wird, wenn der primäre, in dieser Instanz festgelegte, Server nicht erreichbar ist. Geben Sie für den sekundären Server folgende Angaben ein:
   - Name or IP address
   - Port
   - Gemeinsamer geheimer Schlüssel

   Hinweis: Für diesen sekundären RADIUS-Server müssen Sie eine Instanz festlegen.

10. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
11. Konfigurieren Sie den primären und den sekundären RADIUS-Server für die Erkennung des IVE. Folgen Sie hierfür den folgenden Anweisungen.
12. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 379).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 353.

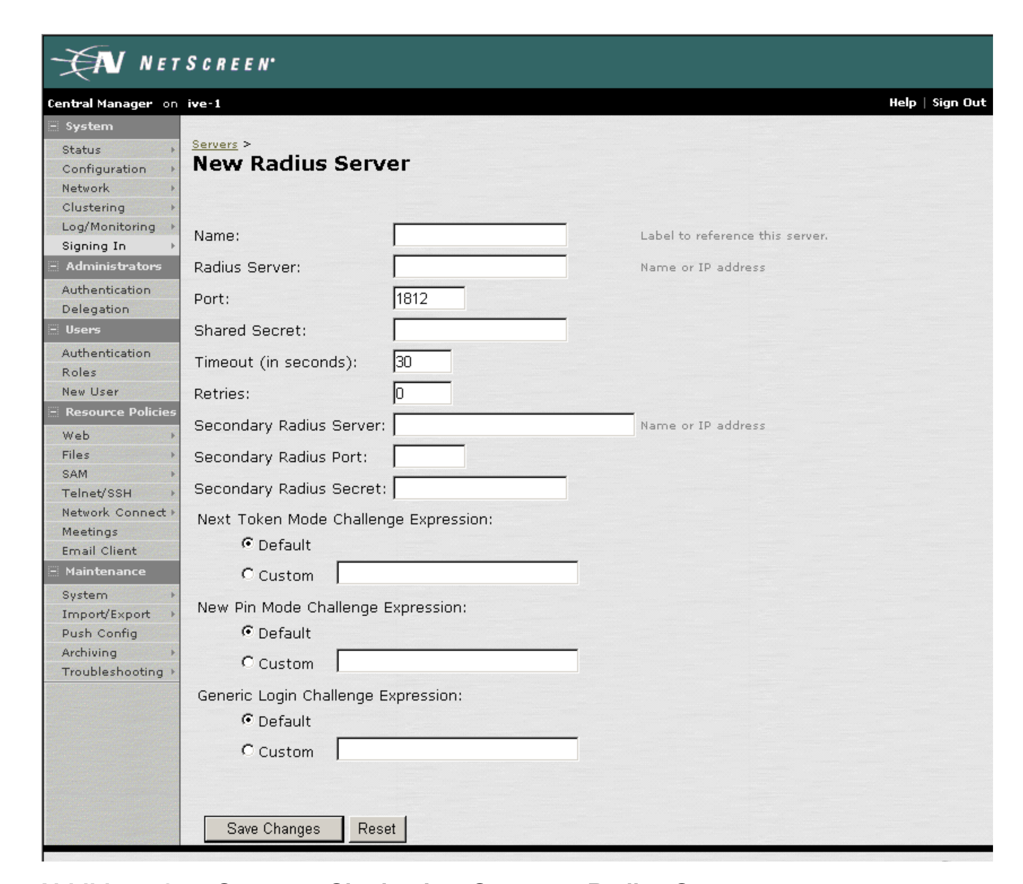


Abbildung 85: System > Signing In > Servers > Radius Server

☑ Konfigurieren des RADIUS-Servers für die Erkennung des IVE

Sie müssen den RADIUS-Server durch folgende Angaben so konfigurieren, dass der IVE-Appliance-Server erkannt wird:

- Hostname der IVE-Appliance.
- Netzwerk-IP-Adresse der IVE-Appliance.
- Clienttyp der IVE-Appliance (sofern vorhanden). Wenn diese Option verfügbar ist, wählen Sie „Single Transaction Server“ oder die entsprechende Option.

- Verschlüsselungstyp für die Authentifizierung der Clientkommunikation. Die ausgewählte Option muss mit dem Clienttyp übereinstimmen.
- Gemeinsamer geheimer Schlüssel, der an der Webkonsole auf der Seite **System > Signing In > Servers > Radius Server** für den RADIUS-Server eingegeben wurde.

Konfigurieren einer Netegrity SiteMinder-Instanz

Die folgenden Themen werden behandelt:

Netegrity SiteMinder – Übersicht

Wenn Sie das IVE für die Authentifizierung von Benutzern mit einem Netegrity SiteMinder-Richtlinienserver konfigurieren, leitet das IVE die Anmeldeinformationen des Benutzers während der Authentifizierung an SiteMinder weiter. Nachdem SiteMinder die Anmeldeinformationen erhalten hat, kann er die Standardauthentifizierung über Benutzername und Kennwort, ACE SecurID-Token oder clientseitige Zertifikate zum Authentifizieren der Anmeldeinformationen verwenden (wie unter „Authentifizierung mit verschiedenen Authentifizierungsschemas" auf Seite 323 erläutert).

Das IVE leitet während der Authentifizierung auch eine geschützte Ressource an SiteMinder weiter, um zu ermitteln, welcher Bereich zum Authentifizieren des Benutzers verwendet werden soll. Wenn das IVE die geschützte Ressource weiterleitet, autorisiert SiteMinder den URL des Benutzers mit dem Bereich, der der Ressource zugeordnet ist, und ermöglicht dem Benutzer den nahtlosen Zugriff auf alle Ressourcen, deren Sicherheitsebenen der vom IVE weitergeleiteten Ressource entsprechen oder eine niedrigere Sicherheitsebene aufweisen (wie unter „Konfigurieren des IVE, um Benutzern Zugriff auf verschiedene geschützte Ressourcen zu gewähren" auf Seite 337 erläutert). Wenn der Benutzer versucht, auf eine Webressource mit einer höheren Sicherheitsebene zuzugreifen, wird die Anforderung entweder von SiteMinder oder vom IVE verarbeitet (wie unter „Erneute Authentifizierung von Benutzern mit unzureichenden Sicherheitsebenen" auf Seite 324 erläutert).

Das IVE ermöglicht die Einzelanmeldung über das IVE bei geschützten SiteMinder-Ressourcen mithilfe von SMSESSION-Cookies. Ein ***SMSESSION-Cookie*** ist ein Sicherheitstoken, das die Anmeldeinformationen und die Sicherheitsebene eines Benutzers speichert. Je nach Konfiguration erstellt entweder der SiteMinder-Web-Agent oder das IVE das SMSESSION-Cookie, um die Anmeldedaten zu speichern. Anschließend wird das SMSESSION-Cookie für folgende Elemente bereitgestellt, damit sich der Benutzer nicht erneut authentifizieren muss, wenn er auf weitere Ressourcen zugreifen möchte:

- **Das IVE**

  Wenn der Benutzer versucht, innerhalb der IVE-Sitzung (z. B. über die IVE-Dateinavigationsseite) auf eine SiteMinder-Ressource zuzugreifen, leitet das IVE das zwischengespeicherte SMSESSION-Cookie zwecks Authentifizierung an den Web-Agent weiter.

- **Den Webbrowser des Benutzers**

  Wenn der Benutzer versucht, außerhalb der IVE-Sitzung (z. B. über sein E-Mail-Konto bei Yahoo!) auf eine SiteMinder-Ressource zuzugreifen, verwendet SiteMinder das zwischengespeicherte SMSESSION-Cookie, das im Webbrowser des Benutzers gespeichert ist, um den Benutzer zu authentifizieren.

Wenn Sie die Option **Automatic Sign-In** aktivieren (Seite 341), kann das IVE auch SMSESSION-Cookies verwenden, um die Einzelanmeldung über eine SiteMinder-Ressource beim IVE zu ermöglichen. Wenn ein Web-Agent die IVE-Anmeldeinformationen sendet, gewährt das IVE dem Benutzer Zugriff (sofern die Anmeldeinformationen authentifiziert werden), ordnet den Benutzer zu dem von Ihnen angegebenen IVE-Bereich und zu der von Ihnen angegebenen Rolle zu.

Sie können einen benutzerdefinierten IVE-Web-Agent (der mit Version 5.5 des Netegrity SDK erstellt wird) oder einen Standard-Web-Agent verwenden, um SMSESSION-Cookies zu erstellen. Beachten Sie bei der jeweiligen Verwendung Folgendes:

- **Benutzerdefinierter IVE-Web-Agent**

  Das IVE authentifiziert Benutzer und generiert SMSESSION-Cookies. Wenn Sie diese Option auswählen, müssen Sie die SiteMinder-Umgebung aktualisieren, sodass Cookies von Drittanbietern akzeptiert werden (Seite 342).

- **Standard-Web-Agent**

  Das IVE sendet Anmeldeinformationen an einen Standard-Web-Agent, den Sie bereits konfiguriert haben. Anschließend erstellt der Web-Agent SMSESSION-Cookies. Wenn Sie diese Option auswählen, können Sie die SecurID New Pin- und Next Token-Modi bzw. die clientseitige Zertifikat-authentifizierung nicht verwenden (Seite 343).

Wichtig:

- Zur Zeit der Drucklegung dieses Dokuments bietet Juniper Networks Unterstützung für Netegrity SiteMinder-Server, Version 6.0 und Version 5.5 mit den standardmäßigen Agentversionen 6, 5QMR5 und 4QMR6.
- SiteMinder speichert die IP-Adresse nicht im SMSESSION-Cookie und kann sie daher nicht an die IVE-Appliance weiterleiten.

- SiteMinder sendet das SMSESSION-Cookie als dauerhaftes Cookie an das IVE. Um ein Höchstmaß an Sicherheit zu gewährleisten, setzt das IVE das dauerhafte Cookie nach Abschluss der Authentifizierung zu einem Sitzungscookie zurück.
- Wenn Sie die Einzelanmeldung zwischen dem IVE und SiteMinder zulassen, ignoriert das IVE sämtliche IVE-Sitzungszeitüberschreitungen und -Leerlaufzeitüberschreitungen und verwendet stattdessen die über den SiteMinder-Bereich festgelegten Sitzungs- und Leerlaufzeitüberschreitungen.

Authentifizierung mit verschiedenen Authentifizierungsschemas

Ein ***Authentifizierungsschema*** bietet in SiteMinder eine Möglichkeit, Anmeldinformationen zu sammeln und die Identität eines Benutzers zu ermitteln. Sie können verschiedene Authentifizierungsschemas erstellen und ihnen jeweils verschiedene Sicherheitsebenen zuordnen. Sie können z. B. zwei Schemas erstellen: eins, das Benutzer nur auf Grundlage ihrer clientseitigen Zertifikate authentifiziert und sie mit einer niedrigen Sicherheitsebene versieht, und ein zweites, das ACE SecurID-Tokenauthentifizierung verwendet und eine höhere Sicherheitsebene bereitstellt. Das IVE funktioniert mit folgenden Arten von SiteMinder-Authentifizierungsschemas:

- **Einfache Authentifizierung über Benutzername und Kennwort**

  Benutzername und Kennwort werden an den SiteMinder-Richtlinienserver weitergeleitet. Der Richtlinienserver kann diese dann selbst authentifizieren oder zur Authentifizierung an einen anderen Server weiterleiten.
- **ACE SecurID-Token-Authentifizierung**

  Der SiteMinder-Richtlinienserver authentifiziert Benutzer auf Grundlage von Benutzername und Kennwort, die von einem ACE SecurID-Token generiert werden.

- **Authentifizierung über clientseitige Zertifikate**

  Der SiteMinder-Richtlinienserver authentifiziert Benutzer auf Grundlage ihrer Anmeldeinformationen des clientseitigen Zertifikats[1]. Wenn Sie diese Authentifizierungsmethode auswählen, zeigt das IVE Benutzern weiterhin die Standardanmeldeseite mit der Eingabeaufforderung für Benutzernamen und Kennwort[2] an. Benutzer können diese Felder jedoch einfach leer lassen und auf **Submit** klicken kann, sofern weder das IVE noch der SiteMinder-Server die Eingabe von Benutzername und Kennwort erfordern.

  Wichtig: Wenn Benutzer anhand dieser Methode authentifiziert werden sollen, müssen Sie das Clientzertifikat über die Registerkarte **System > Certificates > CA Certificates** in das IVE importieren (Seite 190).

Konfigurationsinformationen finden Sie unter:

Erneute Authentifizierung von Benutzern mit unzureichenden Sicherheitsebenen

Während der Konfiguration des IVE müssen Sie eine geschützte Ressource angeben, um die für die SiteMinder-Sitzung des Benutzers zulässige Sicherheitsebene zu steuern (wie unter „Netegrity SiteMinder – Übersicht“ auf Seite 321 erläutert). Wenn ein Benutzer versucht, auf eine Webressource zuzugreifen, die eine höhere Sicherheitsebene erfordert als seine Zugriffsrechte erlauben, kann die erneute Authentifizierung auch über das IVE erfolgen, indem dieses ihn zu einer zwischengeschalteten Seite weiterleitet. Dies setzt jedoch voraus, dass Sie bei der Konfiguration des IVE die Option **Resource for insufficient protection level** aktiviert haben (Seite 346).

1. Die SiteMinder-Authentifizierung über clientseitige Zertifikate läuft getrennt von der IVE-Authentifizierung über clientseitige Zertifikate. Wenn Sie beide Optionen auswählen, nimmt zuerst das IVE die Authentifizierung mithilfe der IVE-Konfigurationsparameter vor. Bei erfolgreichem Verlauf leitet es anschließend die Zertifikatwerte zwecks Authentifizierung an SiteMinder weiter.
2. Wenn Benutzern nicht die IVE-Standardanmeldeseite angezeigt werden soll, können Sie dies mithilfe der Funktion für benutzerdefinierbare Anmeldeseiten ändern, die auf der Juniper Networks-Supportsite zur Verfügung steht.

Die zwischengeschaltete IVE-Seite enthält zwei Optionen:

- **Continue** – Wenn ein Benutzer diese Option auswählt, meldet das IVE ihn bei der aktuellen Sitzung ab und fordert ihn zur Eingabe der Anmeldeinformationen auf, die für die Ressource der höheren Sicherheitsebene[1] erforderlich sind. Wenn die Anmeldeinformationen authentifiziert werden können, leitet es ihn zu der Seite weiter, auf die er ursprünglich zugreifen wollte.
- **Cancel** – Wenn der Benutzer diese Option auswählt, wird er zur vorherigen Seite umgeleitet.

Wenn Sie sich hingegeben festlegen, dass keine erneute Authentifizierung über das IVE erfolgen soll, hängt der erneute Authentifizierungsprozess davon ab, ob der Richtlinienserver einen Authentifizierungsschema-URL an den Benutzer zurückgibt. Wenn auf dem Richtlinienserver Folgendes vorgeht:

- **Keine Rückgabe eines Authentifizierungsschema-URL** – Das IVE sendet dann Meldung über die fehlgeschlagene Validierung an den Benutzer zurück und führt die erneute Authentifizierung über die Standardseite `welcome.cgi` durch. Der Benutzer wird aufgefordert, sich erneut anzumelden, wobei ihm allerdings die ursprüngliche Sicherheitsebene zugeordnet wird und er möglicherweise immer noch keinen Zugriff auf die gewünschte Seite hat.
- **Rückgabe eines Authentifizierungsschema-URLs** – Das IVE leitet den Benutzer zu einem Standard-Web-Agent um, über den die erneute Authentifizierung erfolgen soll.

Informationen zum Konfigurieren des IVE für die erneute Authentifizierung finden Sie unter „Erstellen eines SiteMinder-Authentifizierungsschemas für das IVE“ auf Seite 328.

Ermitteln des Benutzernamens des jeweiligen Benutzers

Wenn verschiedene Authentifizierungsschemas und Anmeldepunkte verfügbar sind, kann das IVE einen Benutzernamen von unterschiedlichen Quellen abrufen, z. B. von einem Richtlinienserverheader, einem Zertifikat-attribut oder von der IVE-Anmeldeseite. Im Folgenden werden die verschiedenen Methoden aufgelistet, die ein Benutzer zum Zugreifen auf das IVE anwenden kann, und es wird erläutert, wie dabei das IVE jeweils den entsprechenden Benutzernamen ermittelt. Wenn ein Benutzer Folgendes vornimmt:

---

1. Wenn der Benutzer die Hostprüfung oder Cachebereinigung ausführt und die Anmeldeinformationen nicht eingibt, wenn das IVE ihn zur erneuten Authentifizierung auffordert, wird die Hostprüfung oder Cachebereinigung auf dem System des Benutzers ausgeführt, bis die IVE-Sitzung des Benutzers abläuft.

- **Anmeldung über die IVE-Standardanmeldeseite**

  Das IVE überprüft zuerst den vom Richtlinienserver im zugehörigen Antwortheader `OnAuthAccept` zurückgegebenen Benutzernamen. Wenn SiteMinder keinen Benutzernamen definiert, verwendet das IVE den vom Benutzer bei der Anmeldung eingegebenen Benutzernamen. Wenn jedoch weder von SiteMinder noch vom Benutzer ein Benutzername bereitgestellt wird, weil sich der Benutzer mit einem Clientzertifikat authentifiziert, verwendet das IVE den vom Richtlinienserver festgelegten Wert `UserDN`.

- **Automatische Anmeldung beim IVE mit SiteMinder-Anmeldeinformationen**

  Das IVE überprüft zuerst den vom Richtlinienserver im zugehörigen Antwortheader `OnAuthAccept` zurückgegebenen Benutzernamen. Wenn SiteMinder keinen Benutzernamen definiert, überprüft das IVE das SMSESSON-Cookie. Wenn SiteMinder den Antwortheader oder das SMSESSION-Cookie jedoch nicht mit einem Benutzernamen auffüllt, verwendet das IVE den im SMSESSION-Cookie enthaltenen Wert `UserDN`.

Nachdem das IVE den zu verwendenden Benutzernamen ermittelt hat, speichert es diesen Benutzernamen im zugehörigen Sitzungscache und verweist darauf, wenn ein Benutzer auf weitere Ressourcen zugreifen möchte (wie unter „Netegrity SiteMinder – Übersicht“ auf Seite 321 erläutert).

Damit stets der richtige Benutzername an das IVE zurückgegeben wird, sollten Sie die Antwort `OnAuthAccept` auf dem SiteMinder-Richtlinienserver entsprechend konfigurieren (wie unter „Erstellen eines Regel-/Antwortpaares zur Weiterleitung von Benutzernamen an das IVE“ auf Seite 332 erläutert).

Konfigurieren von SiteMinder für die Zusammenarbeit mit dem IVE

Im Folgenden wird erläutert, wie Sie einen SiteMinder-Richtlinienserver für die Zusammenarbeit mit dem IVE konfigurieren. Es handelt sich hierbei jedoch nicht um vollständige Konfigurationsanweisungen für SiteMinder. Diese Anweisungen dienen lediglich dazu, Sie beim Einrichten von SiteMinder für die Zusammenarbeit mit dem IVE zu unterstützen. Detaillierte Informationen zur Konfiguration von SiteMinder finden Sie in der Dokumentation zu Ihrem SiteMinder-Richtlinienserver.

Hinweis: Die hier aufgeführten Anweisungen beziehen sich auf den SiteMinder-Richtlinienserver, Version 5.5. Bei Verwendung einer anderen Produktversion können die Anweisungen geringfügig abweichen.

Zum Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver müssen Sie folgende Aufgaben durchführen:

1. Konfigurieren des IVE als Web-Agent auf SiteMinder (Seite 327)
2. Erstellen eines SiteMinder-Authentifizierungsschemas für das IVE (Seite 328)
3. Erstellen einer SiteMinder-Domäne für das IVE (Seite 331)
4. Erstellen eines SiteMinder-Bereichs für das IVE (Seite 331)
5. Erstellen eines Regel-/Antwortpaares zur Weiterleitung von Benutzernamen an das IVE (Seite 332)
6. Erstellen einer SiteMinder-Richtlinie für die Domäne (Seite 335)

☑ Konfigurieren des IVE als Web-Agent auf SiteMinder

In SiteMinder filtert ein ***Agent*** Benutzeranforderungen, um Zugriffssteuerungen zu erzwingen. Wenn ein Benutzer z. B. eine geschützte Ressource anfordert, wird er vom Agent zur Eingabe von Anmeldeinformationen auf der Grundlage eines bestimmten Authentifizierungsschemas aufgefordert. Anschließend werden die Anmeldeinformationen an einen SiteMinder-Richtlinienserver gesendet. Ein ***Web-Agent*** ist ein Agent, der mit einem Webserver kooperiert. Beim Konfigurieren von SiteMinder für die Zusammenarbeit mit dem IVE müssen Sie das IVE als Web-Agent konfigurieren.

So konfigurieren Sie das IVE als Web-Agent auf dem SiteMinder-Richtlinienserver:

1. Wählen Sie auf der SiteMinder-Verwaltungsoberfläche die Registerkarte **System** aus.
2. Klicken Sie mit der rechten Maustaste auf **Agents**, und wählen Sie **Create Agent** aus.
3. Geben Sie einen Namen für den Web-Agent und (optional) eine Beschreibung ein. Beachten Sie, dass Sie diesen Namen eingeben müssen, wenn Sie einen SiteMinder-Bereich erstellen (Seite 331) und das IVE konfigurieren (Seite 339).
4. Sie müssen das Kontrollkästchen **Support 4.x agents** für die Kompatibilität mit dem IVE aktivieren.
5. Aktivieren Sie unter **Agent Type** die Option **SiteMinder**, und wählen Sie dann in der Dropdownliste den Eintrag **Web Agent** aus. Sie müssen diese Einstellung für die Kompatibilität mit dem IVE auswählen.
6. Geben Sie unter **IP Address or Host Name** den Namen oder die IP-Adresse des IVE ein.

7. Geben Sie in den Feldern **Shared Secret** einen geheimen Schlüssel für den Web-Agent ein, und bestätigen Sie diesen. Beachten Sie, dass Sie diesen geheimen Schlüssel beim Konfigurieren des IVE eingeben müssen (Seite 339).
8. Klicken Sie auf **OK**.

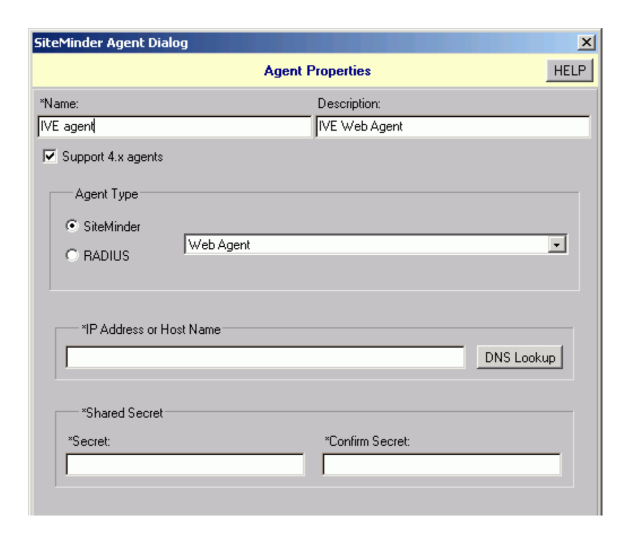


Abbildung 86: SiteMinder Agent Dialog

☑ Erstellen eines SiteMinder-Authentifizierungsschemas für das IVE

Ein ***Authentifizierungsschema*** bietet in SiteMinder eine Möglichkeit, Anmeldinformationen zu sammeln und die Identität eines Benutzers zu ermitteln.

So konfigurieren Sie ein SiteMinder-Authentifizierungsschema für das IVE:

1. Wählen Sie auf der SiteMinder-Verwaltungsoberfläche die Registerkarte **System** aus.
2. Klicken Sie mit der rechten Maustaste auf **Authentication Schemes**, und wählen Sie **Create Authentication Scheme** aus.
3. Geben Sie einen Namen für das Schema und (optional) eine Beschreibung ein. Beachten Sie, dass Sie diesen Namen beim Konfigurieren des SiteMinder-Bereichs eingeben müssen (Seite 332).

4. Wählen Sie unter **Authentication Scheme Type** eine der folgenden Optionen aus:
   - **Basic Template**
   - **HTML Form Template**
   - **SecurID HTML Form Template**[1]
   - **X509 Client Cert Template**
   - **X509 Client Cert and Basic Authentication**

   Wichtig:
   - Das IVE unterstützt nur die hier aufgelisteten Authentifizierungsschematypen.
   - Sie müssen die Option **HTML Form Template** auswählen, wenn die erneute Authentifizierung über das IVE erfolgen soll (wie unter „Erneute Authentifizierung von Benutzern mit unzureichenden Sicherheitsebenen“ auf Seite 324 beschrieben).
   - Wenn Sie **X509 Client Cert Template** oder **X509 Client Cert and Basic Authentication** auswählen, müssen Sie das Zertifikat über die Registerkarte **System > Certificates > CA Certificates** in das IVE importieren (Seite 190).
5. Geben Sie eine Sicherheitsebene für das Schema ein. Beachten Sie, dass diese Sicherheitsebene auf den SiteMinder-Bereich übertragen wird, den Sie diesem Schema zuordnen (Seite 332).
6. Aktivieren Sie **Password Policies Enabled for this Authentication Scheme**, wenn Sie Benutzer, die Ressourcen mit einer höheren Sicherheitsebene anfordern als es die jeweiligen Zugriffsrechte erlauben, erneut authentifizieren möchten.
7. Geben Sie auf der Registerkarte **Scheme Setup** die für den jeweiligen Authentifizierungsschematyp erforderlichen Optionen ein. Wenn das IVE Benutzer, die Ressourcen mit einer höheren Sicherheitsebene anfordern als es die entsprechenden Zugriffsrechte erlauben, erneut authentifizieren soll, müssen Sie die folgenden Einstellungen vornehmen:
   - Geben Sie unter **Server Name** den Hostnamen des IVE ein (z. B. vertrieb.firmenname.net).
   - Aktivieren Sie das Kontrollkästchen **Use SSL Connection**.
   - Geben Sie unter **Target** den im ersten Schritt dieser Aufzählung definierten Anmelde-URL des IVE und den Parameter „ive=1“ ein (z. B. „/highproturl?ive=1“).

---

1. Wenn Sie die SecurID-Authentifizierung verwenden, müssen Sie die Option `SecurID HTML Form Template` (anstelle von `SecurID Template`) auswählen. Durch Auswählen dieser Option kann der Richtlinienserver ACE-Anmeldungsfehlercodes an das IVE senden.

Hinweis: Wenn Sie Änderungen speichern, wird `ive=1` nicht mehr für das Ziel angezeigt. Das ist richtig. Der Richtlinienserver fügt `ive=1` in den vollständigen Authentifizierungsschema-URL ein, den er an das IVE sendet, wie auf der Registerkarte **Advanced** im Feld **Parameter** ersichtlich ist.

- Deaktivieren Sie das Kontrollkästchen **Allow Form Authentication Scheme to Save Credentials**.
- Nehmen Sie keinen Eintrag im Feld **Additional Attribute List** vor.

8. Klicken Sie auf **OK**.

Wichtig: Informationen zum Konfigurieren des IVE für die Verwendung mehrerer Authentifizierungsschemas finden Sie unter „Konfigurieren des IVE für die Verwendung mehrerer Authentifizierungsschemas“ auf Seite 336.

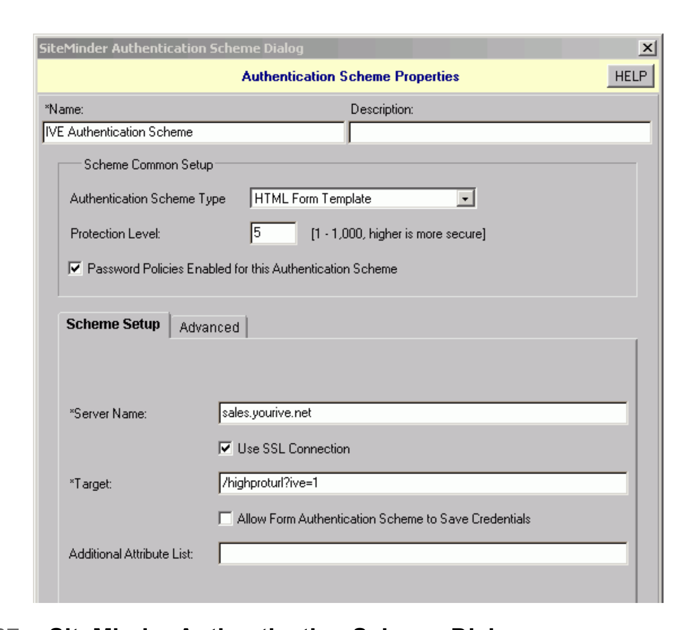


Abbildung 87: **SiteMinder Authentication Scheme Dialog**

☑ Erstellen einer SiteMinder-Domäne für das IVE

In SiteMinder ist eine ***Richtliniendomäne*** eine logische Gruppierung von Ressourcen, die einem oder mehreren Benutzerverzeichnissen zugeordnet sind. Richtliniendomänen umfassen Bereiche, Antworten und Richtlinien. Beim Konfigurieren des IVE für die Zusammenarbeit mit SiteMinder müssen Sie den IVE-Benutzern Zugriff auf eine SiteMinder-Ressource innerhalb eines Bereichs gewähren und den Bereich anschließend in einer Domäne gruppieren.

Zum Konfigurieren einer SiteMinder-Domäne für das IVE wählen Sie auf der SiteMinder-Verwaltungsoberfläche die Registerkarte **System** aus. Klicken Sie dann mit der rechten Maustaste auf **Domains**, und wählen Sie **Create Domain** aus. Oder klicken Sie auf **Domains**, und wählen Sie eine vorhandene SiteMinder-Domäne aus. Beachten Sie, dass Sie dieser Domäne einen Bereich hinzufügen müssen (Seite 331).

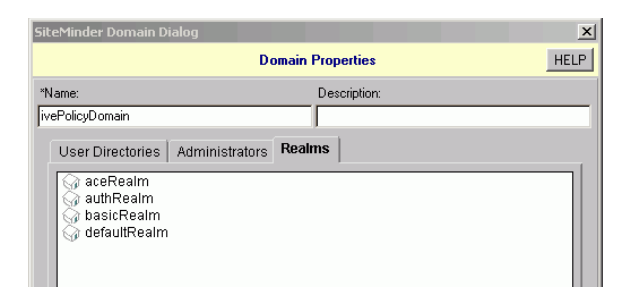


Abbildung 88: SiteMinder Domain Dialog

☑ Erstellen eines SiteMinder-Bereichs für das IVE

In SiteMinder ist ein ***Bereich*** ein Cluster von Ressourcen innerhalb einer Richtliniendomäne, die nach Sicherheitsanforderungen gruppiert sind. Beim Konfigurieren von SiteMinder für die Zusammenarbeit mit dem IVE müssen Sie Bereiche definieren, um festzulegen, auf welche Ressourcen die IVE-Benutzer zugreifen dürfen.

So konfigurieren Sie einen SiteMinder-Bereich für das IVE:

1. Wählen Sie auf der SiteMinder-Verwaltungsoberfläche die Registerkarte **Domains** aus.
2. Erweitern Sie die Domäne, die Sie für das IVE erstellt haben (Seite 331).
3. Klicken Sie mit der rechten Maustaste auf **Realms**, und wählen Sie **Create Realm** aus.

4. Geben Sie einen Namen für den Bereich und (optional) eine Beschreibung ein.
5. Wählen Sie im Feld **Agent** den Web-Agent aus, den Sie für das IVE erstellt haben (Seite 327).
6. Geben Sie im Feld **Resource Filter** eine geschützte Ressource ein. Diese Ressource erbt die im zugehörigen Authentifizierungsschema angegebene Sicherheitsebene. Geben Sie für die Standard-sicherheitsebene Folgendes ein: `/ive-authentication`. Beachten Sie, dass Sie diese Ressource beim Konfigurieren des IVE eingeben müssen (Seite 339).
7. Wählen Sie aus der Liste **Authentication Schemes** das Schema aus, das Sie für das IVE erstellt haben (Seite 328).
8. Klicken Sie auf **OK**.

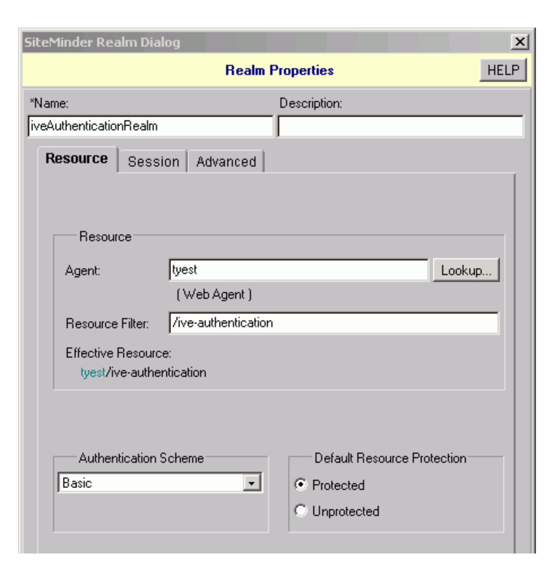


Abbildung 89: **SiteMinder Realm Dialog**

☑ Erstellen eines Regel-/Antwortpaares zur Weiterleitung von Benutzernamen an das IVE

In SiteMinder können Sie ***Regeln*** verwenden, um Antworten auszulösen, wenn Authentifizierungs- oder Autorisierungsereignisse stattfinden. Eine ***Antwort*** leitet Benutzerattribute, DN-Attribute, statischen Text oder benutzerdefinierte aktive Antworten vom SiteMinder-Richtlinienserver an einen SiteMinder-Agent weiter. Beim Konfigurieren von SiteMinder für die Zusammenarbeit mit dem IVE müssen Sie eine Regel erstellen, die ausgelöst wird, wenn sich ein Benutzer erfolgreich authentifiziert.

Anschließend müssen Sie eine entsprechende Antwort erstellen, die den Benutzernamen des jeweiligen Benutzers an den IVE-Web-Agent weiterleitet.

So erstellen Sie eine neue Regel:

1. Wählen Sie auf der SiteMinder-Verwaltungsoberfläche die Registerkarte **Domains** aus.
2. Erweitern Sie die Domäne, die Sie für das IVE erstellt haben (Seite 331), und erweitern Sie dann **Realms**.
3. Klicken Sie mit der rechten Maustaste auf den Bereich, den Sie für das IVE erstellt haben (Seite 331), und wählen Sie **Create Rule under Realm** aus.
4. Geben Sie einen Namen für die Regel und (optional) eine Beschreibung ein.
5. Aktivieren Sie unter **Action** das Optionsfeld **Authentication Events**, und wählen Sie dann in der Dropdownliste den Eintrag **OnAuthAccept** aus.
6. Wählen Sie **Enabled** aus.
7. Klicken Sie auf **OK**.

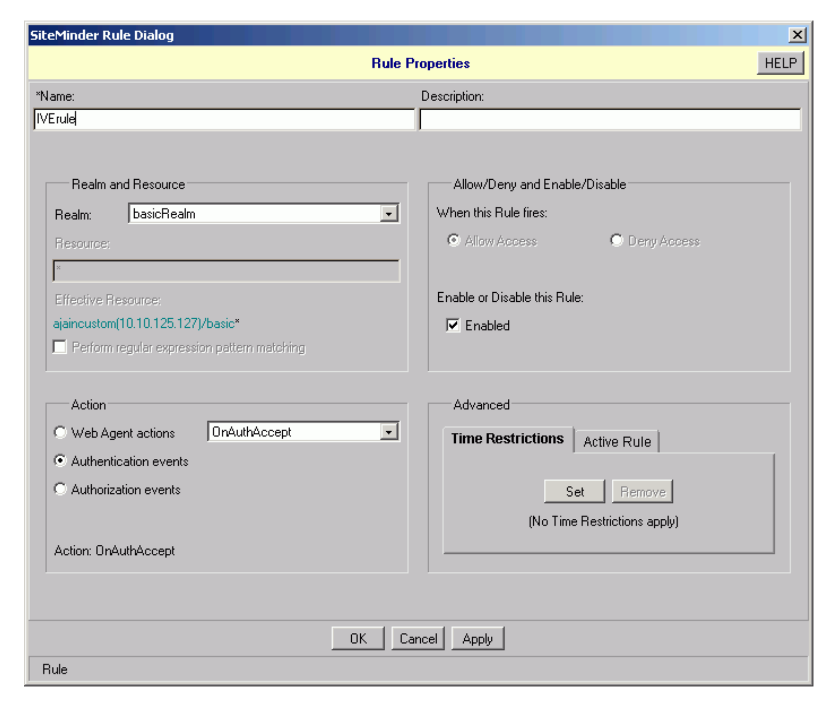


Abbildung 90: **SiteMinder Rule Dialog**

So erstellen Sie eine neue Antwort:

1. Wählen Sie auf der SiteMinder-Verwaltungsoberfläche die Registerkarte **Domains** aus.
2. Erweitern Sie die Domäne, die Sie für das IVE erstellt haben (Seite 331).
3. Klicken Sie mit der rechten Maustaste auf **Responses**, und wählen Sie **Create Response** aus.
4. Geben Sie einen Namen für die Antwort und (optional) eine Beschreibung ein.
5. Wählen Sie **SiteMinder** aus, und wählen Sie dann den IVE-Web-Agent aus (Seite 327).
6. Klicken Sie auf **Create**.
7. Wählen Sie aus der Liste **Attribute** den Eintrag **WebAgent-HTTP-Header-Variable** aus.
8. Aktivieren Sie unter **Attribute Kind** die Option **Static**.
9. Geben Sie im Feld **Variable Name** Folgendes ein: **IVEUSERNAME**.

10. Klicken Sie auf **OK**.

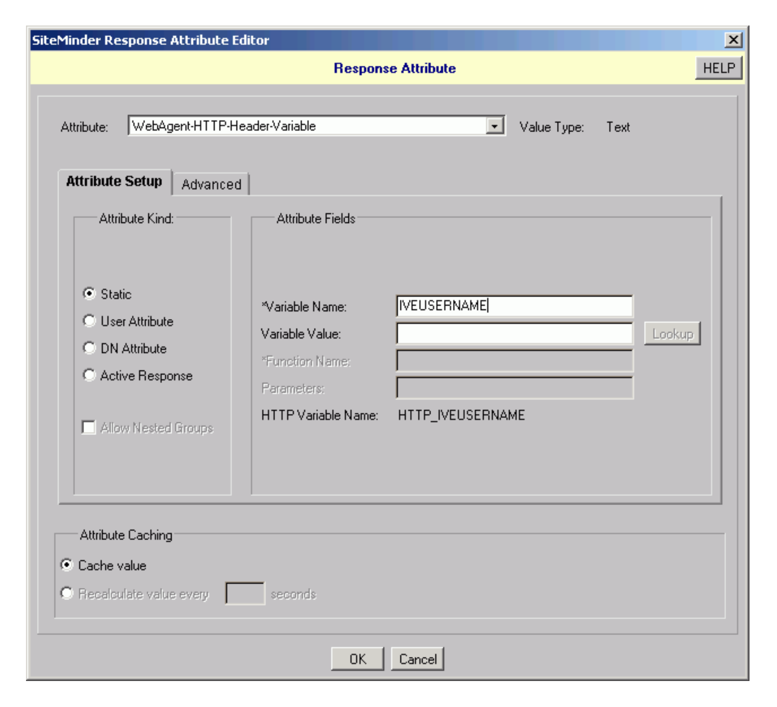


Abbildung 91: **SiteMinder Response Attribute Editor**

☑ Erstellen einer SiteMinder-Richtlinie für die Domäne

In SiteMinder ordnet eine ***Richtlinie*** Benutzern Regeln zu. Zum Konfigurieren einer SiteMinder-Richtlinie für eine Domäne wählen Sie auf der SiteMinder-Verwaltungsoberfläche die Registerkarte **Domains** aus. Wählen Sie dann die Domäne aus, der Sie eine Richtlinie hinzufügen möchten, klicken Sie mit der rechten Maustaste auf **Policies**, und wählen Sie **Create Policy** aus.

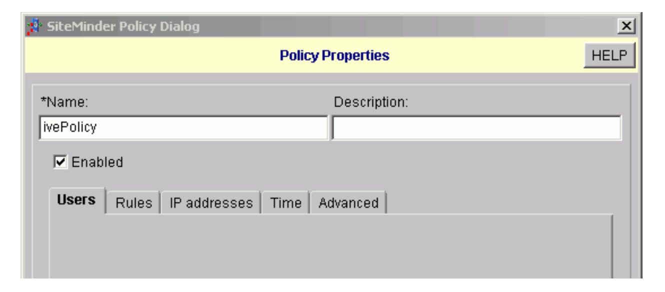


Abbildung 92: SiteMinder Policy Dialog

Konfigurieren des IVE für die Zusammenarbeit mit SiteMinder

Dieser Abschnitt enthält die folgenden Anweisungen für das Konfigurieren des IVE für die Zusammenarbeit mit einem SiteMinder-Richtlinienserver:

☑ Konfigurieren des IVE für die Verwendung mehrerer Authentifizierungsschemas

Zum Konfigurieren des IVE für die Verwendung mehrerer SiteMinder-Authentifizierungsschemas gehen Sie folgendermaßen vor:

1. Konfigurieren Sie die Authentifizierungsschemas auf dem SiteMinder-Richtlinienserver. Anweisungen hierfür finden Sie unter „Erstellen eines SiteMinder-Authentifizierungsschemas für das IVE“ auf Seite 328.
2. Erstellen Sie für jedes zu verwendende Authentifizierungsschema jeweils eine IVE-Instanz des Richtlinienservers. Anweisungen hierfür finden Sie unter „Festlegen einer Netegrity SiteMinder-Serverinstanz“ auf Seite 338.
3. Ordnen Sie jeder IVE-Instanz ein anderes SiteMinder-Authentifizierungs-schema zu. (Nehmen Sie diese Zuordnungen durch Verweise vor. Geben Sie beim Konfigurieren des IVE eine geschützte Ressource ein, die dem zu verwendenden SiteMinder-Authentifizierungs-schema entspricht.)
4. Ordnen Sie jeder IVE-Instanz einen anderen IVE-Anmelde-URL zu. Anweisungen hierfür finden Sie unter „Erstellen und Konfigurieren von Anmelderichtlinien“ auf Seite 268.

Während der Produktion meldet sich der Benutzer mit einem der URLs beim IVE an. Das IVE sendet die dem URL zugeordnete geschützte Ressource an SiteMinder, und SiteMinder ermittelt anhand der Ressource, welcher Schematyp zum Authentifizieren des Benutzers verwendet werden soll. Das IVE sammelt dann die für das Authentifizierungsschema erforderlichen Anmeldinformationen und leitet sie zur Authentifizierung an SiteMinder weiter.

☑ Konfigurieren des IVE, um Benutzern Zugriff auf verschiedene geschützte Ressourcen zu gewähren

Wenn Sie das IVE konfigurieren möchten, um Benutzern Zugriff auf verschiedene geschützte SiteMinder-Ressourcen (nach Zuordnung und unterschiedlichen Sicherheitsebenen) zu gewähren, müssen Sie folgendermaßen vorgehen:

1. Definieren Sie die vom SiteMinder-Server zu schützenden Ressourcen. Jede dieser Ressourcen erbt eine Sicherheitsebene eines zugehörigen SiteMinder-Authentifizierungsschemas. Anweisungen hierfür finden Sie unter „Erstellen eines SiteMinder-Bereichs für das IVE" auf Seite 331.
2. Erstellen Sie für jede geschützte Ressource und die entsprechende Sicherheitsebene, die Sie zulassen möchten, jeweils eine IVE-Instanz des Richtlinienservers. Anweisungen hierfür finden Sie unter „Festlegen einer Netegrity SiteMinder-Serverinstanz" auf Seite 338.
3. Ordnen Sie jeder IVE-Instanz einen anderen Ressourcenfilter auf Bereichsebene zu. (Geben Sie beim Konfigurieren des IVE eine geschützte Ressource ein, die dem SiteMinder-Ressourcenfilter zugeordnet ist, den Sie zulassen möchten.)
4. Ordnen Sie jeder IVE-Instanz einen anderen IVE-Anmelde-URL zu. Achten Sie beim Definieren des URLs darauf, dass der Pfadabschnitt des URLs mit dem SiteMinder-Ressourcenfilter übereinstimmt. Sie können beispielsweise folgende URLs definieren:

   `https://mitarbeiter.eigenefirma.com/sales`

   `https://mitarbeiter.eigenefirma.com/engineering`

   Wenn sich Benutzer über den ersten URL anmelden, wird ihnen der Zugriff auf die geschützte Ressource „Sales" gewährt, und wenn sie sich über den zweiten URL anmelden, wird ihnen der Zugriff auf die geschützte Ressource „Engineering" gewährt.

   Zum Definieren einer Standardressource (`ive-authentication`) geben Sie im Pfadabschnitt des URLs ein Sternchen (*) ein. Anweisungen hierfür finden Sie unter „Erstellen und Konfigurieren von Anmelderichtlinien" auf Seite 268.

Während der Produktion meldet sich der Benutzer mit einem der URLs beim IVE an. Das IVE extrahiert die geschützte Ressource aus dem URL und authentifiziert den Benutzer anhand des entsprechenden Bereichs.

☑ Festlegen einer Netegrity SiteMinder-Serverinstanz

Im IVE können Sie unterschiedliche Instanzen des SiteMinder-Servers konfigurieren. Bei einer ***Instanz*** handelt es sich um eine Reihe von Konfigurationsoptionen, mit denen die Interaktion zwischen dem IVE und dem SiteMinder-Richtlinienserver definiert wird. Beachten Sie, dass jede Instanz die Konfigurationseinstellungen desselben SiteMinder-Richtlinienservers umfassen muss.

So legen Sie eine Netegrity SiteMinder-Serverinstanz fest:

1. Wählen Sie in der Webkonsole die Optionen **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **SiteMinder Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Konfigurieren Sie den Server mit den in Tabelle 2 beschriebenen Einstellungen.
4. Klicken Sie auf **Save Changes**.
5. Legen Sie ggf. erweiterte SiteMinder-Konfigurationsoptionen mithilfe der in Tabelle 3 beschriebenen Einstellungen fest.
6. Geben Sie die IVE-Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 381).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 353.

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Name	Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
Policy Server	Geben Sie den Namen oder die IP-Adresse des SiteMinder-Richtlinienservers ein, den Sie zum Authentifizieren von Benutzern verwenden möchten.
Backup Server(s), Failover Mode	Geben Sie eine durch Kommas getrennte Liste von Richtlinien-sicherungsservern ein (optional). Wählen Sie dann einen Failover-Modus aus: • Wählen Sie **Yes** aus, damit die IVE-Appliance den Hauptrichtlinienserver verwendet, sofern dieser betriebsbereit ist. • Wählen Sie **No** aus, damit die IVE-Appliance einen Lastenausgleich zwischen allen Richtlinienservern vornimmt.
Secret, Agent Name	Geben Sie den gemeinsamen geheimen Schlüssel und den Agentnamen ein (wie unter „Konfigurieren des IVE als Web-Agent auf SiteMinder“ auf Seite 327 angegeben). Berücksichtigen Sie bei diesen Angaben die Groß- und Kleinschreibung.
On logout, redirect to	Geben Sie einen URL an, zu dem Benutzer bei der Abmeldung vom IVE umgeleitet werden (optional). Wenn Sie dieses Feld leer lassen, wird Benutzern die IVE-Standardanmeldeseite angezeigt. **Wichtig:** Das Feld **On logout, redirect to** wurde aus Gründen der Abwärtskompatibilität in dieser Produktversion berücksichtigt, in zukünftigen Versionen wird es jedoch nicht mehr enthalten sein. Wenn Sie Benutzer nach der Abmeldung zu einer anderen Anmeldeseite umleiten möchten, empfiehlt es sich dringend, stattdessen die Funktion für benutzer-definierbare Anmeldeseiten zu verwenden (Seite 274).
Protected Resource	Geben Sie die unter „Erstellen eines SiteMinder-Bereichs für das IVE“ auf Seite 331 angegebene geschützte Ressource an. Das IVE verwendet diesen URL, um die Sicherheitsebene des Benutzers für die jeweilige Sitzung festzulegen. Wenn die Benutzer sich an dem URL „*“ (IVE-Standardanmeldeseite) anmelden, geben Sie „/ive-authentication“ ein, um die Sicherheitsebene auf den IVE-Standardwert festzulegen. Hinweis: Sie müssen einen Schrägstrich (/) vor der Ressource eingeben (z. B. „/ive-authentication“).

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Resource Action	(Schreibgeschützt) Bei neuen SiteMinder-Serverinstanzen legt das IVE die Ressourcenaktion auf GET fest. Wenn die SiteMinder-Instanz von einer 3.x-Instanz aktualisiert wird, verwendet das IVE die zuvor ausgewählte Ressourcenaktion (z. B. GET, POST oder PUT). Wenn Sie eine vorhandene Ressourcenaktion in GET ändern möchten, müssen Sie die alte SiteMinder-Serverinstanz löschen und anschließend eine neue Instanz erstellen, die GET verwendet.
SMSESSION-Cookieeinstellungen:	
Cookie Domain	Geben Sie die Cookiedomäne des IVE ein. (Eine ***Cookiedomäne*** ist eine Domäne, in der die Cookies des Benutzers aktiv sind. Das IVE sendet Cookies an den Browser des Benutzers in dieser Domäne.) Beachten Sie folgende Punkte: • Mehrere Domänen müssen durch Kommas getrennt werden. Beispiel: vertrieb.eigeneorg.com, marketing.eigeneorg.com • Bei Domänennamen wird die Groß- und Kleinschreibung berücksichtigt. • Es dürfen keine Platzhalterzeichen verwendet werden. Wenn Sie z. B. „.juniper.net“ definieren, muss der Benutzer über „http://ive.juniper.net“ auf das IVE zugreifen, um sicherzustellen, dass das zugehörige SMSESSION-Cookie an das IVE zurückgesendet wird.
Protocol	(Schreibgeschützt) Gibt an, dass das IVE Cookies mit dem HTTPS-Protokoll an den Webbrowser des Benutzers sendet.
Cookie Provider Domain	Geben Sie die Internetdomäne(n) ein, an die das IVE das SMSESSION-Cookie sendet. Hierfür gelten dieselben Richtlinien, die bereits für das Feld **Cookie Domain** erörtert wurden. (Eine ***Domäne des Cookieanbieters*** ermöglicht die Einzelanmeldung bei mehreren Cookiedomänen. Dabei sind beim Navigieren von einer Domäne zu einer anderen stets die Informationen eines Benutzers verfügbar.) Wenn Sie für einen Cookieanbieter die Einzelanmeldung über mehrere Cookiedomänen aktiviert haben, geben Sie den Namen des Cookieanbieters ein. Andernfalls geben Sie die Domäne(n) der Web-Agents ein, für die eine Einzelanmeldung erfolgen soll. Beispiel: .juniper.net, .netscreen.com
Protocol	Wählen Sie **HTTPS**, um Cookies sicher zu senden, sofern andere Web-Agents für den Empfang sicherer Cookies eingerichtet sind, oder wählen Sie **HTTP**, um Cookies ungesichert zu senden.

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
SiteMinder-Authentifizierungseinstellungen:	
Automatic Sign-In	Aktivieren Sie das Kontrollkästchen **Automatic Sign-In**, wenn Benutzer, die über ein gültiges SMSESSION-Cookie verfügen, automatisch beim IVE angemeldet werden sollen. Wählen Sie dann den Authentifizierungsbereich aus, dem die Benutzer zugeordnet werden. Beachten Sie bei Auswahl dieser Option Folgendes: • Wenn sich ein Benutzer automatisch an einem URL anmeldet, der mehreren Authentifizierungsbereichen zugeordnet ist, meldet das IVE den Benutzer an dem in der IVE-Webkonsole auf der Registerkarte **System > Signing In > Servers > [SiteMinder-Server]** angegebenen Bereich an (nicht an dem URL, der auf der Registerkarte **System > Signing In > Sign-in Policies** angegeben ist). • Wenn die Sicherheitsebene, die dem SMSESSION-Cookie eines Benutzers zugeordnet ist, von der Sicherheitsebene des IVE-Bereichs abweicht, verwendet das IVE die Sicherheitsebene, die dem Cookie zugeordnet ist. • Damit die Einzelanmeldung von einem anderen Web-Agent beim IVE möglich ist, muss das IVE ein vorhandenes SMSESSION-Cookie überprüfen, das von einem Standard-Web-Agent erstellt wurde. • Die einzigen Einschränkungen auf Bereichs- und Rollenebene, die das IVE im Rahmen der Funktion **Automatic Sign in** unterstützt, sind Überprüfungen der IP-Adresse, des Browsers und der Begrenzungen für gleichzeitig angemeldete Benutzer. Nicht unterstützte Einschränkungen auf Rollen- und Bereichsebene umfassen Zertifikat- und Kennworteinschränkungen (die nicht für automatisch angemeldete Benutzer gelten) sowie Hostprüfungs- und Cachebereinigungs-einschränkungen. • Das IVE bietet im Hinblick auf Administratorrollen keine Unterstützung für die Funktion **Automatic Sign in**. Diese Funktion ist nur für Endbenutzer verfügbar.
To assign user roles, use this authentication realm	Wählen Sie einen Authentifizierungsbereich für automatisch angemeldete Benutzer aus. Das IVE ordnet dem Benutzer eine Rolle auf Grundlage der im ausgewählten Bereich definierten Rollenzuordnungsregeln zu. **Hinweis:** Wenn Sie Benutzern Rollen auf Grundlage von Benutzernamen zuordnen möchten, finden Sie unter „Ermitteln des Benutzernamens des jeweiligen Benutzers" Informationen zu dem vom IVE verwendeten Benutzernamen.

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Authenticate using custom agent	Wählen Sie diese Option aus, wenn die Authentifizierung über den benutzerdefinierten Web-Agent des IVE erfolgen soll. Beachten Sie, dass Sie bei Auswahl dieser Option außerdem folgende Aufgaben durchführen müssen: • Aktualisieren aller Standard-Web-Agents mit dem entsprechenden Siteminder Agent Quarterly Maintenance Release (QMR), damit die vom IVE erstellten Cookies akzeptiert werden. Wenn Sie SiteMinder-Web-Agents, Version 5, ausführen, verwenden Sie den auf der Netegrity-Website verfügbaren QMR5-Hotfix. • Festlegen des Attributs **AcceptTPCookie** (Cookie von Drittanbietern akzeptieren) in der Konfigurationsdatei des Web-Agent (**webagent.conf**) auf „yes“ oder in der Windows-Registrierung für den IIS-Webserver auf „1“. Der Speicherort des Attributs hängt von der verwendeten SiteMinder-Version und vom verwendeten Webserver ab. Weitere Informationen finden Sie in der Dokumentation zu Ihrem SiteMinder-Server.

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Authenticate using HTML form post	Wählen Sie diese Option aus, wenn Sie die Benutzeranmeldeinformationen an einen bereits konfigurierten Standard-Web-Agent senden möchten, statt direkt mit dem SiteMinder-Richtlinienserver zu kommunizieren. Wenn Sie diese Option auswählen, kommuniziert der Web-Agent mit dem Richtlinienserver, um die jeweilige Anmeldeseite zu ermitteln, die dem Benutzer angezeigt werden soll. Damit Sie das IVE so konfigurieren können, dass es „wie ein Browser fungiert", der Anmeldeinformationen an den Standard-Web-Agent sendet, müssen Sie die unten definierten Informationen eingeben. Sie können diese Informationen problemlos finden, indem Sie folgendermaßen vorgehen: 1 Öffnen Sie einen Webbrowser, und geben Sie den URL des Standard-Web-Agent ein, den Sie verwenden möchten. Beispiel: http://webagent.juniper.net 2 Notieren Sie sich den URL der angezeigten SiteMinder-Anmeldeseite. Beispiel: http://webagent.juniper.net/siteminderagent/forms/login.fcc?TYPE=33554433&REALMOID=06-2525fa65-5a7f-11d5-9ee0-0003471b786c&GUID=&SMAUTHREASON=0&TARGET=SMhttp%3a%2f%2fwebagent%2ejuniper%2enet%2fportal%2findex%2ejsp 3 Extrahieren Sie die entsprechenden Informationen aus dem URL, um die folgenden Felder auszufüllen. **Hinweis:** • Sie können die SecurID New Pin- und Next Token-Modi, die clientseitige Zertifikatauthentifizierung und SNMP-Traps nicht in Verbindung mit der Option **Authenticate using HTML form post** verwenden. • Die Option **Authorize While Authenticating** kann nicht in Verbindung mit der Option **HTML form post** angewendet werden. • Sie können Benutzer zwar mithilfe dieser Option authentifizieren, wenn Sie sie jedoch auch autorisieren möchten, müssen Sie die Option **Authenticate using custom agent** auswählen.
Target	URL auf dem externen, Netegrity-fähigen Webserver. Im URL der Anmeldeseite des Web-Agent wird das Ziel im Anschluss an „&TARGET=SM" angezeigt. In dem oben aufgeführten URL (Seite 343) lautet das Ziel beispielsweise wie folgt: http%3a%2f%2fwebagent%2ejuniper%2enet%2fportal%2findex%2ejsp Nach dem Konvertieren der Sonderzeichen (%3a=Doppelpunkt, %2f=umgekehrter Schrägstrich, %2e=Punkt) lautet das endgültige Ziel wie folgt: http://webagent.juniper.net/portal/index.jsp

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Protocol	Protokoll für die Kommunikation zwischen IVE und dem angegebenen Web-Agenten. Verwenden Sie HTTP für die nicht sichere Kommunikation oder HTTPS für die sichere Kommunikation. Im URL der Anmeldeseite des Web-Agent wird zuerst das Protokoll angezeigt. In dem oben aufgeführten URL (Seite 343) wird beispielsweise HTTP verwendet.
Web Agent	Name des Web-Agenten, von dem das IVE SMSESSION-Cookies abrufen soll. Eine IP-Adresse kann in diesem Feld nicht eingegeben werden. (Wenn die IP-Adresse als Web-Agent angegeben wird, können einige Browser keine Cookies akzeptieren.) Im URL der Anmeldeseite des Web-Agent wird der Web-Agent im Anschluss an das Protokoll angezeigt. In dem oben aufgeführten URL (Seite 343) heißt der Web-Agent beispielsweise folgendermaßen: webagent.juniper.net
Port	Port 80 für HTTP oder Port 443 für HTTPS.
Path	Pfad der Anmeldeseite des Web-Agenten. Beachten Sie, dass der Pfad mit einem umgekehrten Schrägstrich (/) beginnen muss. Im URL der Anmeldeseite des Web-Agent wird der Pfad im Anschluss an den Web-Agent angezeigt. In dem oben aufgeführten URL (Seite 343) lautet der Pfad beispielsweise wie folgt: /siteminderagent/forms/login.fcc
Parameters	Post-Parameter, die bei der Anmeldung eines Benutzers gesendet werden. Zu den häufig verwendeten SiteMinder-Variablen zählen `_ _USER_ _`, `_ _PASS_ _` und `_ _TARGET_ _`. Diese Variablen werden durch den vom Benutzer auf der Anmeldeseite des Web-Agent eingegebenen Benutzernamen und durch das Kennwort sowie durch den im Feld **Target** angegebenen Wert ersetzt. Es handelt sich hierbei um die Standardparameter für **login.fcc**. Wenn Sie Anpassungen vorgenommen haben, müssen Sie diese Parameter möglicherweise ändern.

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
If authentication fails, redirect to	Geben Sie einen alternativen URL für Benutzer ein, die sich über den Mechanismus zur automatischen Anmeldung beim IVE anmelden (Seite 341). Das IVE leitet Benutzer zum angegebenen URL um, wenn das IVE die Benutzer nicht authentifizieren kann und vom SiteMinder-Richtlinienserver keine Antwort zum Umleiten empfangen wird. Wenn Sie dieses Feld leer lassen, werden die Benutzer aufgefordert, sich erneut beim IVE anzumelden. **Hinweis:** • Benutzer, die sich über die IVE-Anmeldeseite anmelden, werden grundsätzlich wieder zurück zur IVE-Anmeldeseite umgeleitet, wenn keine Authentifizierung erfolgen kann. • Wenn Sie die Option für die Anpassung der Oberfläche verwenden (Seite 274), beachten Sie, dass das IVE noch in zwei weiteren Fällen auf die Seite `welcome.cgi` umleitet. Sie müssen beide Sonderfälle in Ihrer benutzerdefinierten Seite berücksichtigen: Ablauf der Sitzungs- oder Leerlaufhöchstdauer: /dana-na/auth/welcome.cgi?p=timed-out Fehlgeschlagene Cookievalidierung: /dana-na/auth/welcome.cgi?p=failed
Verwenden von SiteMinder für die Autorisierung:	
Authorize requests against SiteMinder policy server	Aktivieren Sie diese Option, wenn die Regeln des SiteMinder-Richtlinienservers für die Autorisierung der Benutzeranforderungen von Webressourcen verwendet werden sollen. Wenn Sie diese Option auswählen, müssen Sie in SiteMinder die entsprechenden Regeln erstellen, die mit dem Servernamen und einem Schrägstrich beginnen, z. B.: „www.yahoo.com/“, „www.yahoo.com/*“ und „www.yahoo.com/r/f1“. Weitere Informationen finden Sie in der Dokumentation zu Ihrem SiteMinder-Server.
If authorization fails, redirect to	Geben Sie einen alternativen URL ein, zu dem Benutzer umgeleitet werden, wenn das IVE die Benutzer nicht autorisieren kann und vom SiteMinder-Richtlinienserver keine Antwort zum Umleiten empfangen wird. Wenn Sie dieses Feld leer lassen, werden die Benutzer aufgefordert, sich erneut beim IVE anzumelden.

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Resource for insufficient protection level	Geben Sie eine Ressource des Web-Agent ein, zu der das IVE die Benutzer umleitet, wenn sie nicht über die erforderlichen Berechtigungen verfügen. Wenn ein Benutzer auf eine Ressource zugreift, die eine höhere Sicherheitsebene als das SMSESSION-Cookie des Benutzers aufweist, wird eine gesicherte Anmeldeseite geöffnet. Nach der erneuten Authentifizierung erhält er dann ein SMSESSION-Cookie mit einer höheren Sicherheitsebene und wird zu einer Webseite umgeleitet. Der jeweils vom IVE angezeigte Webseitentyp richtet sich nach der von Ihnen verwendeten Methode für die erneute Authentifizierung von Benutzern*: • **A standard Web agent with "FCCCompatMode = yes"** Wenn Sie den Kompatibilitätsmodus für den Formularanmelde-informationen-Collector des Web-Agent (Forms Credential Collector, FCC)** auf „yes“ festlegen, werden die Benutzer zu der von Ihnen im Feld **Resource for insufficient protection level** angegebenen Seite umgeleitet. Beachten Sie folgende Punkte: - Sie müssen die Benutzer zu einer Seite des Standard-Web-Agent umleiten. Das IVE kann den Benutzer nicht zu der Ressource weiterleiten, auf die er ursprünglich zugreifen wollte. - Sie müssen dabei nicht den gesamten URL der Ressource (z. B. „https://vertrieb.eigenefirma.com/,DanaInfo=www.stdwebagent.com+index.html“), sondern nur die Ressource („index.html“) eingeben. • **A standard Web agent with "FCCCompatMode = no"** Wenn Sie den Kompatibilitätsmodus für den Formularanmelde-informationen-Collector des Web-Agent (Forms Credential Collector, FCC)** auf „yes“ festlegen, werden die Benutzer zu der von Ihnen im Feld **Resource for insufficient protection level** angegebenen Seite umgeleitet. Wenn Sie dieses Feld leer lassen, wird der Benutzer zu der Ressource umgeleitet, auf die er ursprünglich zugreifen wollte. • **Das IVE** Wenn die erneute Authentifizierung der Benutzer über das IVE erfolgt, werden die Benutzer zu einer zwischengeschalteten IVE-Seite umgeleitet (siehe „Erneute Authentifizierung von Benutzern mit unzureichenden Sicherheitsebenen“ auf Seite 324). Wenn das IVE den Benutzer zu der Ressource umleiten soll, auf die er ursprünglich zugreifen wollte, müssen Sie in der IVE-Webkonsole auf der Seite **Users > Roles > [Rolle] > General > Session Options** die Option **Browser request follow through** aktivieren. (Wenn Sie dieses Feld leer lassen und die Option **Browser request follow through** nicht aktivieren, leitet das IVE den Benutzer zu der IVE-Seite um, die der Benutzer als Standardlesezeichen festgelegt hat.)

Tabelle 2: Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
	* Informationen zum Festlegen einer Methode für die erneute Authentifizierung finden Sie unter „Erstellen eines SiteMinder-Authentifizierungsschemas für das IVE“ auf Seite 328. ** Wenn ein Benutzer eine geschützte Ressource anfordert, wird er von SiteMinder an einen Formularanmeldeinformationen-Collector (FCC) weitergeleitet, der dann auf dem Richtlinienserver ein Webformular zum Erfassen der Anmeldeinformationen aufruft.
Ignore authorization for files with extensions	Geben Sie Dateierweiterungen ein, die den Dateitypen entsprechen, für die keine Autorisierung erforderlich ist. Sie müssen die Erweiterung jedes einzelnen Dateityps eingeben, der ignoriert werden soll, und diese durch Kommas trennen. Geben Sie beispielsweise „.gif, .jpeg, .jpg, .bmp“ ein, um verschiedene Bilddateitypen zu ignorieren. Es dürfen keine Platzhalterzeichen (wie *, *.* oder .*) verwendet werden, um eine ganze Gruppe von Dateitypen zu ignorieren.

Tabelle 3: Erweiterte Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Poll Interval	Geben Sie das Intervall ein, nach dessen Ablauf das IVE den SiteMinder-Richtlinienserver auf neue Schlüssel überprüft.
Max. Connections	Steuert die maximale Anzahl gleichzeitiger Verbindungen, die das IVE mit dem Richtlinienserver herstellen kann. Die Standardeinstellung ist 20.
Max. Requests/ Connection	Steuert die maximale Anzahl der Anforderungen, die von der Richtlinienserververbindung verarbeitet werden, bevor das IVE die Verbindung trennt. Sie können diese Einstellung ggf. ändern, um die Leistungsfähigkeit zu erhöhen. Die Standardeinstellung ist 1000.
Idle Timeout	Steuert die maximale Anzahl der Minuten, die sich eine Verbindung mit dem Richtlinienserver im Leerlauf befinden kann (wobei die Verbindung keine Anforderungen verarbeitet), bevor das IVE die Verbindung trennt. Die Standardeinstellung „none“ gibt an, dass es keine zeitliche Begrenzung gibt.

Tabelle 3: Erweiterte Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Authorize while Authenticating	Legt fest, dass das IVE unmittelbar nach der Authentifizierung auf dem Richtlinienserver nach Benutzerattributen suchen soll, um zu ermitteln, ob der Benutzer tatsächlich authentifiziert wurde. Wenn beispielsweise der Netegrity-Server Benutzer auf der Grundlage einer LDAP-Servereinstellung authentifiziert, können Sie diese Option auswählen, um anzugeben, dass das IVE Benutzer über den Netegrity-Server authentifizieren und anschließend über den LDAP-Server autorisieren soll, bevor den Benutzern der Zugriff gewährt wird. Wenn der Benutzer nicht authentifiziert oder autorisiert werden kann, wird er zu der auf dem Richtlinienserver konfigurierten Seite umgeleitet. **Hinweis:** • Wenn Sie diese Option nicht auswählen und die Autorisierungsoptionen mithilfe des Richtlinienserver-Konfigurationsprogramms auf der Registerkarte **Policy Users > Exclude** festgelegt haben, kann sich ein Benutzer, dem Sie den Zugriff verweigert haben, erfolgreich auf dem IVE authentifizieren. Erst wenn der Benutzer versucht, auf eine geschützte Ressource zuzugreifen, überprüft das IVE seine Autorisierungsrechte und verweigert ihm den Zugriff. • Das IVE sendet sowohl zur Autorisierung als auch zur Authentifizierung dieselbe Ressource an den Richtlinienserver. • Diese Option wird nicht in Verbindung mit den Optionen **Authenticate using HTML form post** (Seite 343) und **Automatic sign-in** (Seite 341) unterstützt.
Enable Session Grace Period, Validate cookie every N seconds	Sie können den Aufwand, der mit dem Überprüfen des SMSESSION-Cookies eines Benutzers bei jeder Benutzeranforderung derselben Ressource verbunden ist, erheblich reduzieren, indem Sie angeben, dass das IVE das Cookie für einen bestimmten Zeitraum als gültig betrachten soll. In dieser Zeit geht das IVE davon aus, dass das zwischengespeicherte Cookie gültig ist, sodass keine erneute Überprüfung über den Richtlinienserver erfolgt. Wenn Sie diese Option nicht auswählen, überprüft das IVE das SMSESSION-Cookie des Benutzers bei jeder Anforderung. Beachten Sie, dass der hier eingegebene Wert keinen Einfluss auf die Überprüfung von Sitzungs- oder -Leerlaufzeitüberschreitungen hat.

Tabelle 3: Erweiterte Netegrity SiteMinder-Konfigurationsoptionen

Option	Beschreibung
Ignore Query Data	Wenn ein Benutzer eine Ressource anfordert, sendet das IVE standardmäßig den gesamten URL für diese Ressource (einschließlich des Abfrageparameters) an den Richtlinienserver, wobei das Ergebnis der Autorisierungsanforderung 10 Minuten lang zwischengespeichert wird. Wählen Sie diese Option aus, damit das IVE (unter der Voraussetzung, dass nur ein anderer Abfrageparameter vorliegt) die zwischengespeicherte Antwort verwendet, statt erneut mit dem Richtlinienserver zu kommunizieren, wenn der Benutzer dieselbe Ressource anfordert, die im zwischengespeicherten URL angegeben ist.
Accounting Port	Der Wert in diesem Feld muss mit dem über die Netegrity Policy Server Management Console eingegebenen Wert für den Accounting Port übereinstimmen. Standardmäßig stimmt dieses Feld mit der Standardeinstellung des Richtlinienservers (44441) überein.
Authentication Port	Der Wert in diesem Feld muss mit dem über die Netegrity Policy Server Management Console eingegebenen Wert für den Authentifizierungsport übereinstimmen. Standardmäßig stimmt dieses Feld mit der Standardeinstellung des Richtlinienservers (44442) überein.
Authorization Port	Der Wert in diesem Feld muss mit dem über die Netegrity Policy Server Management Console eingegebenen Wert für den Autorisierungsport übereinstimmen. Standardmäßig stimmt dieses Feld mit der Standardeinstellung des Richtlinienservers (44443) überein.
Flush Cache	Hiermit kann der Ressourcencache des IVE gelöscht werden, in dem Ressourcenautorisierungsdaten 10 Minuten lang zwischengespeichert werden.

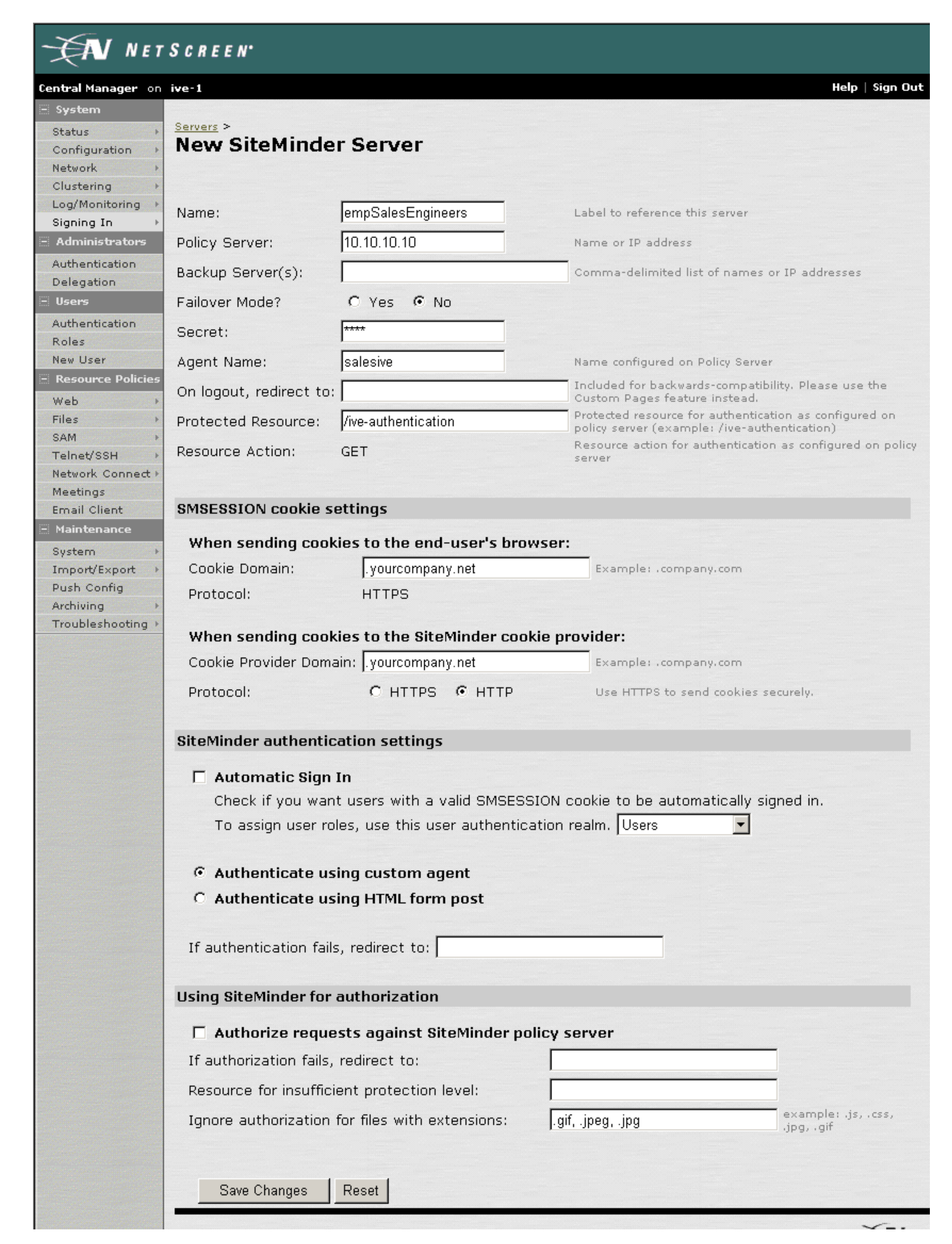


Abbildung 93: System > Signing In > Servers > SiteMinder Server

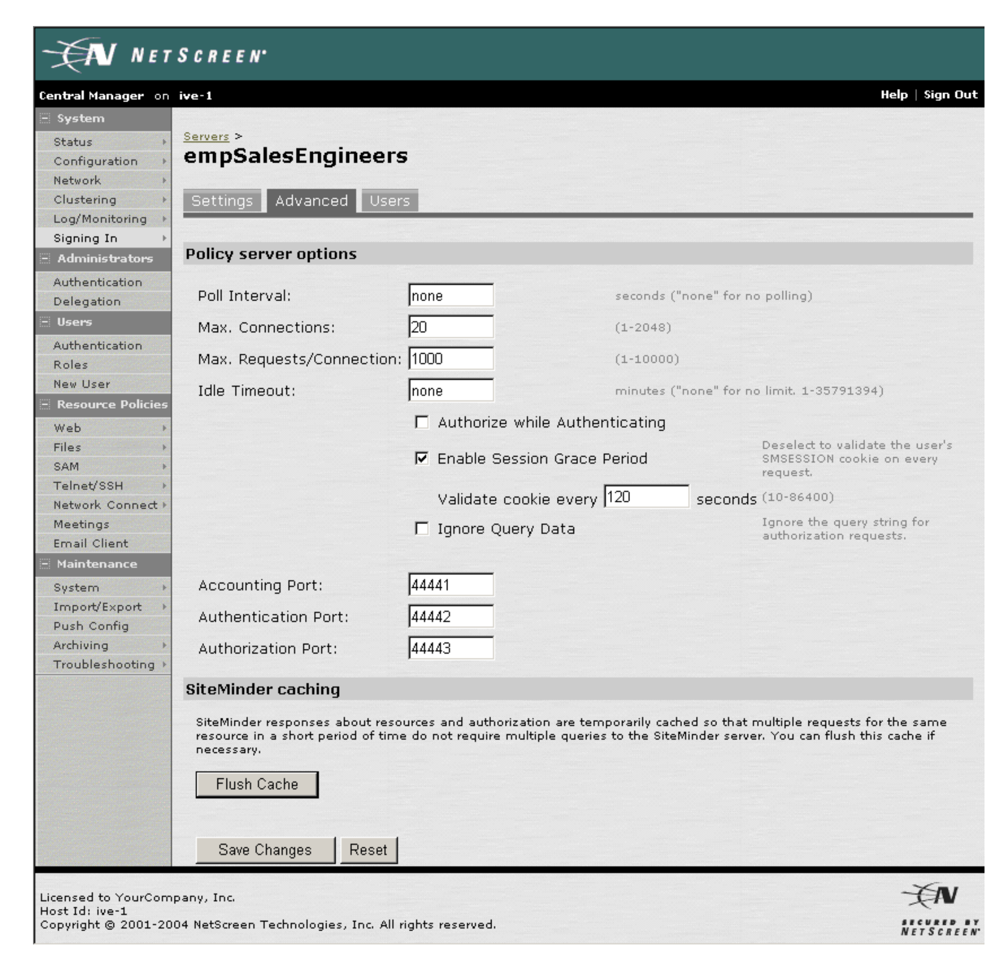


Abbildung 94: System > Signing In > Servers > SiteMinder Server > Advanced

Anzeigen und Löschen von Benutzersitzungen

☑ Anzeigen und Löschen aktiver IVE-Benutzersitzungen

Die Konfigurationsseite für die meisten IVE-Authentifizierungsserver enthält eine Registerkarte **Users**, auf der Sie aktive IVE-Benutzersitzungen anzeigen und löschen können. Auf den folgenden Typen von Authentifizierungsservern wird diese Registerkarte nicht angezeigt:

- **Anonymer Server** – Das IVE kann keine individuellen Sitzungsdaten für Benutzer anzeigen, die sich über einen anonymen Server anmelden, da bei der Benutzeranmeldung über einen anonymen Server keine Benutzernamen oder anderen Anmeldeinformationen erfasst werden.
- **Lokaler IVE-Server** – Das IVE zeigt für lokale IVE-Server statt einer Registerkarte **Users** eine Registerkarte **Local Users** an, auf der Sie Benutzerkonten (anstelle von Benutzersitzungen) hinzufügen und löschen können.

Bei sämtlichen anderen Typen von Authentifizierungsservern können Sie aktive Benutzersitzungen anzeigen und löschen. Folgen Sie hierfür den folgenden Anweisungen.

So zeigen Sie eine aktive Benutzersitzung an oder löschen sie:

1. Wählen Sie in der Webkonsole **System > Signing In > Servers** aus.
2. Klicken Sie in der Liste **Authentication/Authorization Servers** auf die entsprechende Verknüpfung.
3. Klicken Sie auf die Registerkarte **Users**.
4. Führen Sie eine der folgenden Aufgaben durch:
   - Geben Sie im Feld **Show Users Named** einen Benutzernamen ein, und klicken Sie auf **Update**, um nach einem bestimmten Benutzer zu suchen.

     Sie können auch ein Sternchen (`*`) als Platzhalter verwenden, das für eine beliebige Anzahl von Zeichen steht (null, eins oder mehrere). Wenn Sie z. B. nach allen Benutzernamen suchen möchten, die die Buchstaben `jo` enthalten, geben Sie im Feld **Show users named** die Zeichenfolge `*jo*` ein. Bei der Suche wird die Groß- und Kleinschreibung berücksichtigt. Wenn Sie wieder die Gesamtliste der Gruppenkonten anzeigen möchten, geben Sie ein Sternchen (`*`) ein, oder löschen Sie den Feldinhalt, und klicken Sie dann auf **Update**.
   - Geben Sie im Feld **Show N users** eine Zahl ein, und klicken Sie auf **Update**, um die Anzahl von Benutzern anzugeben, die auf der Seite angezeigt werden.

- Aktivieren Sie das Kontrollkästchen neben den jeweiligen Benutzern, und klicken Sie anschließend auf **Delete**, um deren IVE-Sitzungen zu beenden.

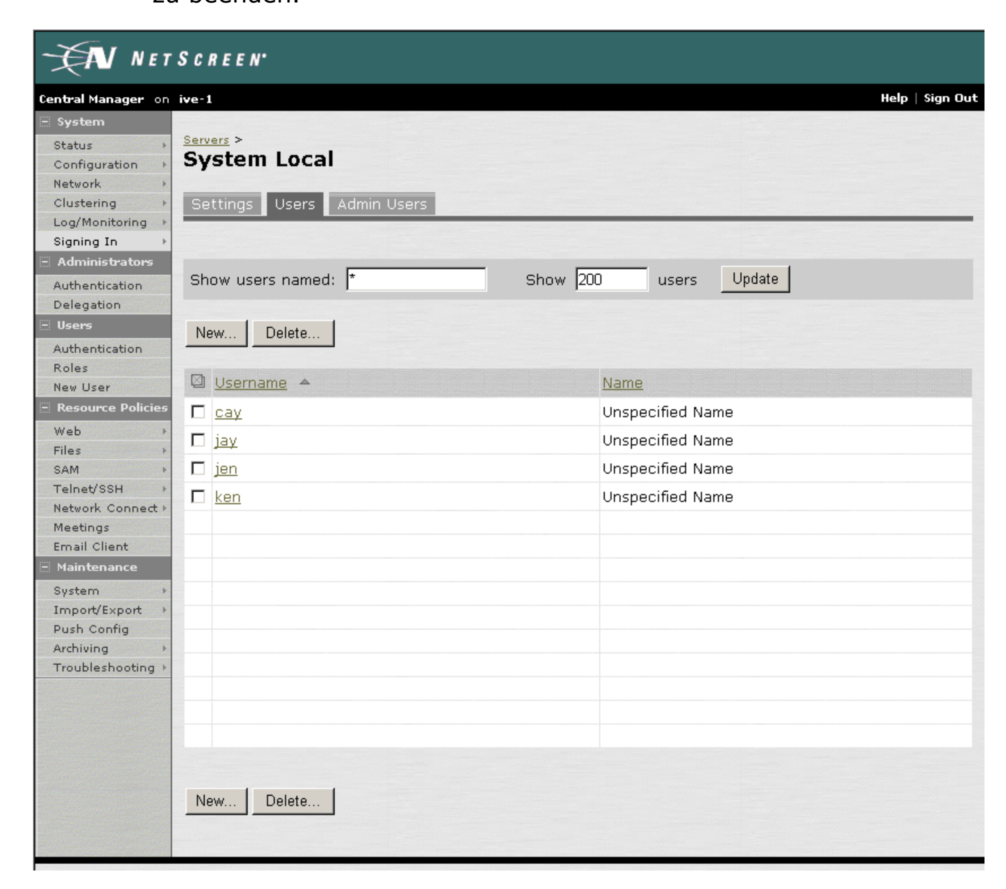


Abbildung 95: **System > Signing In > Servers > [Ausgewählter Server] > Users**

Konfigurieren der Seite „Delegation“

Auf der Seite **Administrators > Delegation** können Sie Administratorberechtigungen (schreibgeschützt, lese- und schreibberechtigt, verweigern) für verschiedene Systemaufgaben wie Netzwerkbetrieb, Einrichtung von Clustern und Protokollierung sowie für die Funktionen zum Verwalten der auf dem System definierten Benutzerrollen festlegen. Weitere Informationen finden Sie unter „Delegierte Administration – Übersicht“ auf Seite 87.

Die Seite **Administrators > Delegation** enthält die folgenden Registerkarten:

Auf den Registerkarten der Seite **Administrators > Delegation**
können Sie die folgenden Aufgaben durchführen:

☑ Erstellen, Ändern und Löschen von Administratorrollen

Wenn Sie zu **Administrators > Delegation** navigieren, wird die Seite **Delegated Admin Roles** angezeigt. Auf dieser Seite können Sie Administratorrollen erstellen, ändern und löschen sowie Standardoptionen für Sitzungen und Benutzeroberfläche für delegierte Administratorrollen festlegen.

So erstellen Sie eine Administratorrolle:

1. Wählen Sie in der Webkonsole die Option **Administrators > Delegation** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie zum Erstellen einer neuen Administratorrolle mit den Standardeinstellungen auf **New Role**.
   - Aktivieren Sie das Kontrollkästchen neben einer vorhandenen Administratorrolle, und klicken Sie auf **Duplicate**, um die Rolle und benutzerdefinierten Berechtigungen zu kopieren. Beachten Sie, dass Sie die Systemstandardrollen (**.Administrators** und **.Read-Only Administrators**) nicht kopieren können.
3. Geben Sie unter **Name** einen Namen (erforderlich) und unter **Description** eine Beschreibung (optional) für die neue Rolle ein, und klicken Sie auf **Save Changes**.
4. Ändern Sie die Rolleneinstellungen nach den Anweisungen in:
   - „Registerkarte „General > Overview““ auf Seite 359
   - „Registerkarte „System““ auf Seite 368
   - „Registerkarte „Users > Roles““ auf Seite 371
   - „Registerkarte „Users > Authentication Realms““ auf Seite 374
   - „Registerkarte „Resource Policies““ auf Seite 377

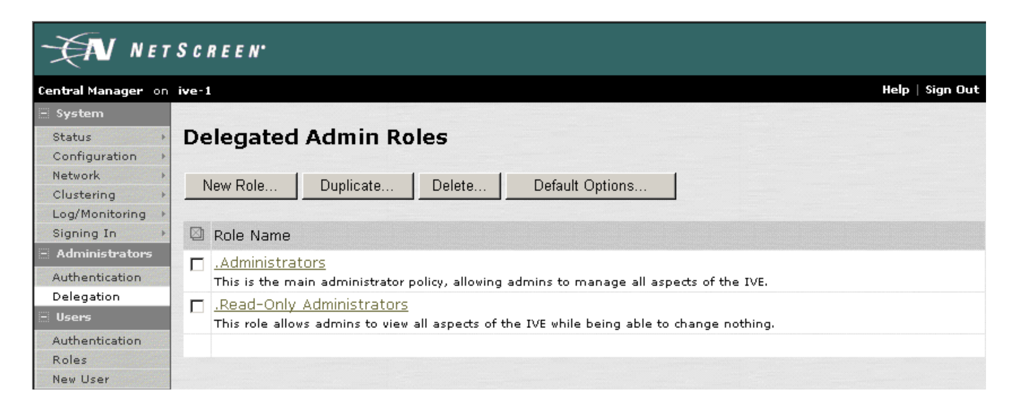


Abbildung 96: Administrators > Delegation

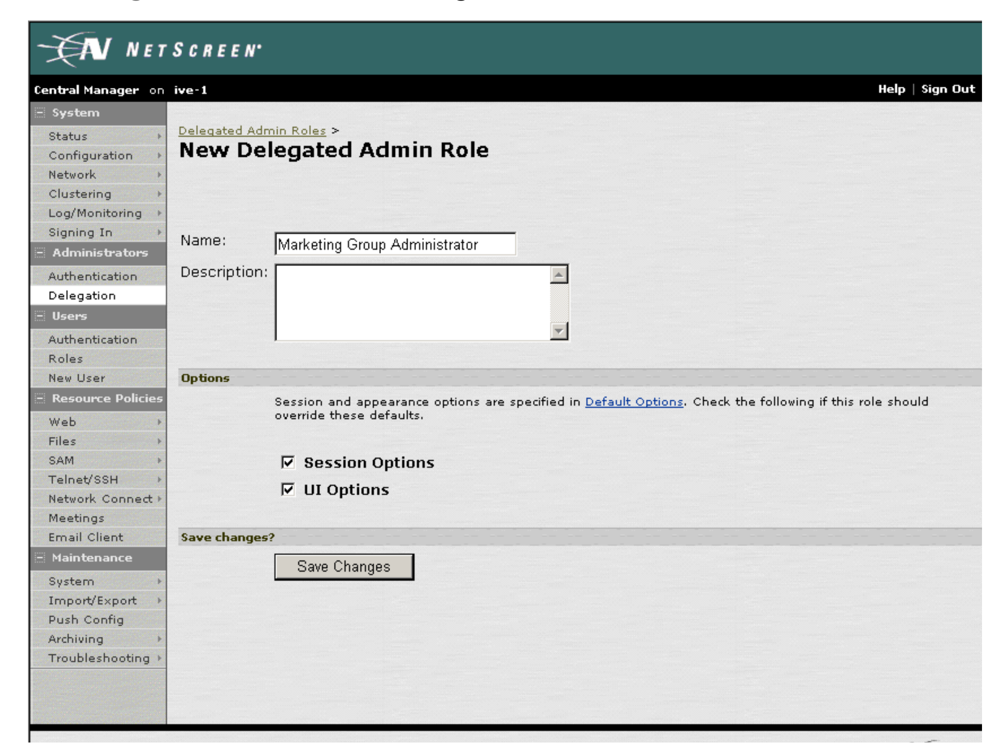


Abbildung 97: Administrators > Delegation > New Role

So ändern Sie eine vorhandene Administratorrolle:

1. Wählen Sie in der Webkonsole die Option **Administrators > Delegation** aus.
2. Klicken Sie auf den Namen der zu ändernden Administratorrolle.
3. Ändern Sie die Rolleneinstellungen nach den Anweisungen in:
   - „Registerkarte „General > Overview““ auf Seite 359
   - „Registerkarte „System““ auf Seite 368
   - „Registerkarte „Users > Roles““ auf Seite 371
   - „Registerkarte „Users > Authentication Realms““ auf Seite 374
   - „Registerkarte „Resource Policies““ auf Seite 377

Hinweis: Wenn Sie eine der Standardadministratorrollen („.Administrators“ oder „.Read-Only Administrators“) von IVE auswählen, können Einstellungen nur auf der Registerkarte **General** geändert werden (da die IVE-Standard-administratorrollen immer auf die Funktionen zugreifen, die über die Registerkarten **System**, **Users** und **Resource Policies** definiert wurden).

So löschen Sie eine vorhandene Administratorrolle:

1. Wählen Sie in der Webkonsole die Option **Administrators > Delegation** aus.
2. Aktivieren Sie das Kontrollkästchen neben der zu löschenden Administratorrolle, und klicken Sie auf **Delete**.
3. Klicken Sie auf **Delete**, um das Entfernen der ausgewählten Rolle zu bestätigen.

Hinweis: Die Rollen „.Administrators“ und „.Read Only Administrators“ können nicht gelöscht werden, da es sich um im IVE definierte Standardrollen handelt.

So definieren Sie die Standardoptionen für alle delegierten Administratorrollen:

1. Wählen Sie in der Webkonsole die Option **Administrators > Delegation** aus.
2. Klicken Sie auf **Default Options**.
3. Ändern Sie anhand der Anweisungen unter „Registerkarte „General > Overview““ auf Seite 359 die Einstellungen auf den Registerkarten **Session Options** und **UI Options**, und klicken Sie auf **Save Changes**. Diese stellen ab jetzt die neuen Standardwerte für alle neuen delegierten Administratorrollen dar.

Registerkarte „General > Overview“

☑ Verwalten allgemeiner Einstellungen und Optionen für Rollen

Auf der Registerkarte **General > Overview** können Sie den Namen und die Beschreibung einer Rolle ändern sowie Sitzungs- und Benutzeroberflächenoptionen an- und ausschalten.

So verwalten Sie allgemeine Einstellungen und Optionen für Rollen:

1. Klicken Sie in der Webkonsole auf **Administrators > Delegation> *Ausgewählte Rolle* > General > Overview**.
2. Erstellen Sie anhand der Felder **Name** und **Description** eine Bezeichnung für die delegierte Administratorrolle.
3. Aktivieren Sie unter **Options** folgende Kontrollkästchen:
    - **Session Options**, um die auf der Registerkarte **General > Session Options** konfigurierten Einstellungen auf die Rolle anzuwenden.
    - **UI Options**, um die auf der Registerkarte **General > UI Options** konfigurierten Einstellungen auf die Rolle anzuwenden.
4. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

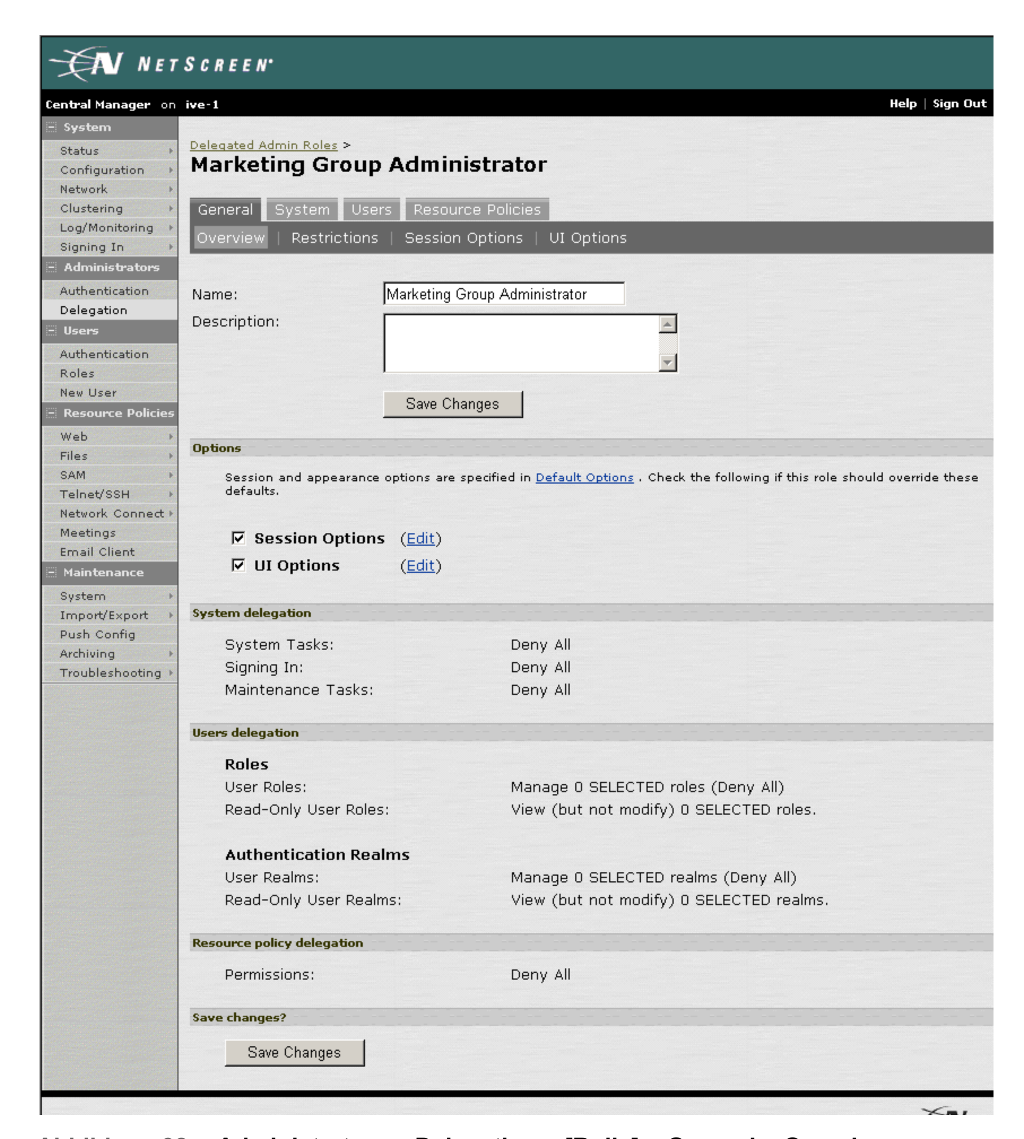


Abbildung 98: **Administrators > Delegation > [Rolle] > General > Overview**

Registerkarte „General > Restrictions“

Legen Sie auf der Registerkarte **General > Restrictions** Zugriffsverwaltungsoptionen für die Rolle fest. Das IVE berücksichtigt diese Einschränkungen, wenn es ermittelt, ob der Rolle ein Administrator zuzuordnen ist. Das IVE ordnet delegierte Administratoren nur dann dieser Rolle zu, wenn sie die angegebenen Einschränkungen erfüllen. Weitere Informationen zur Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 25.

☑ Festlegen von Zugriffsverwaltungsoptionen für die Rolle

So legen Sie Zugriffsverwaltungsoptionen für die Rolle fest:

1. Klicken Sie in der Webkonsole auf **Administrators > Delegation> *Ausgewählte Rolle* > General > Restrictions**.
2. Klicken Sie auf die Registerkarte, die der Option entspricht, die Sie für die Rolle konfigurieren möchten:
   - Source IP (Seite 584)
   - Browser (Seite 585)
   - Certificate (Seite 587)
   - Host Checker (Seite 590)

   Für die Rolle kann eine beliebige Anzahl von Zugriffsverwaltungsoptionen konfiguriert werden. Wenn ein Administrator nicht alle Einschränkungen erfüllt, dann ordnet das IVE den delegierten Administrator der Rolle nicht zu.
3. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

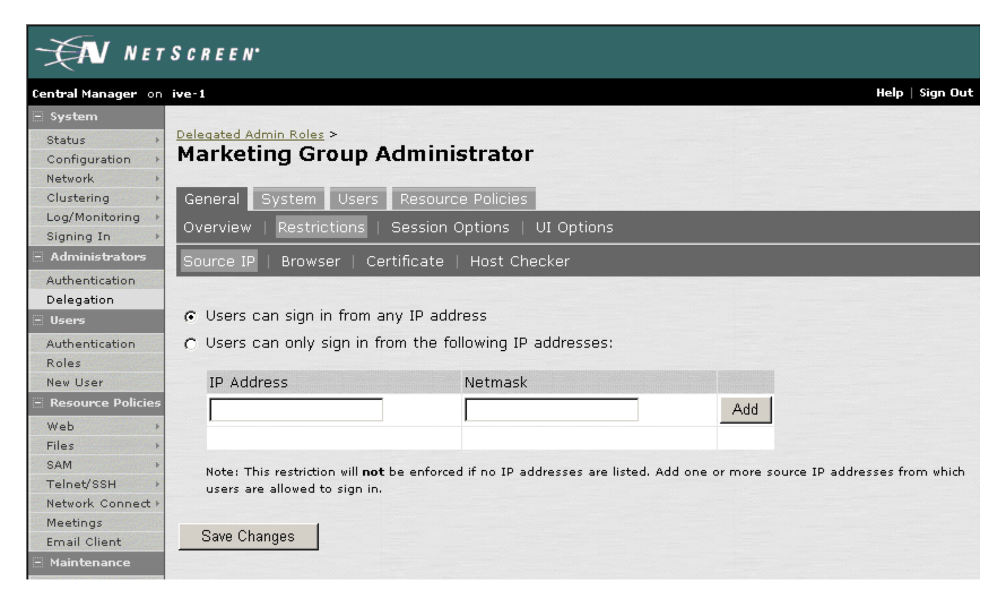


Abbildung 99: Administrators > Delegation > [Rolle] > General > Restrictions > Source IP

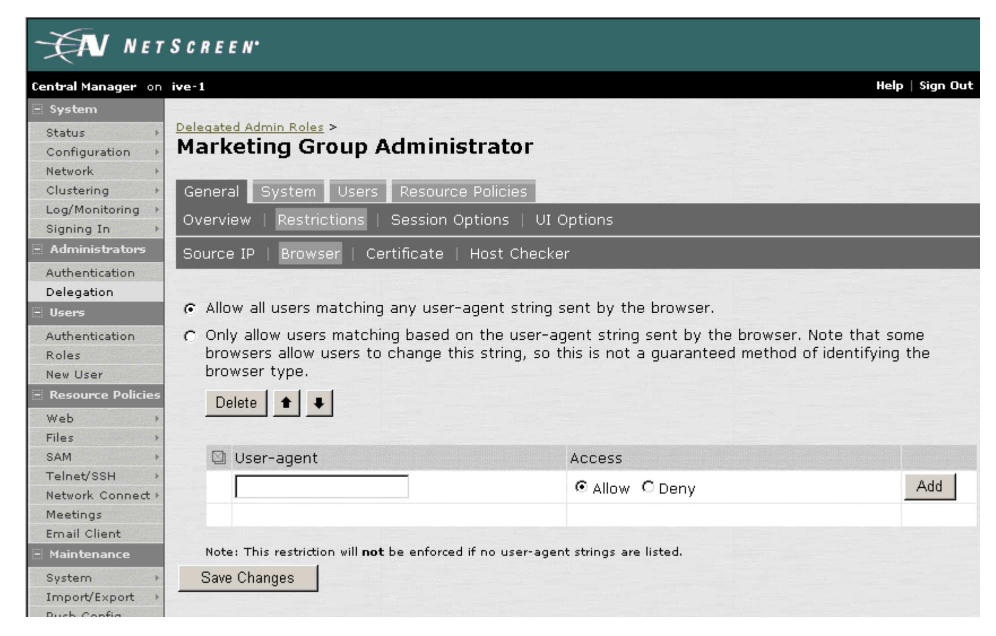


Abbildung 100: Administrators > Delegation > [Rolle] > General > Restrictions > Browser

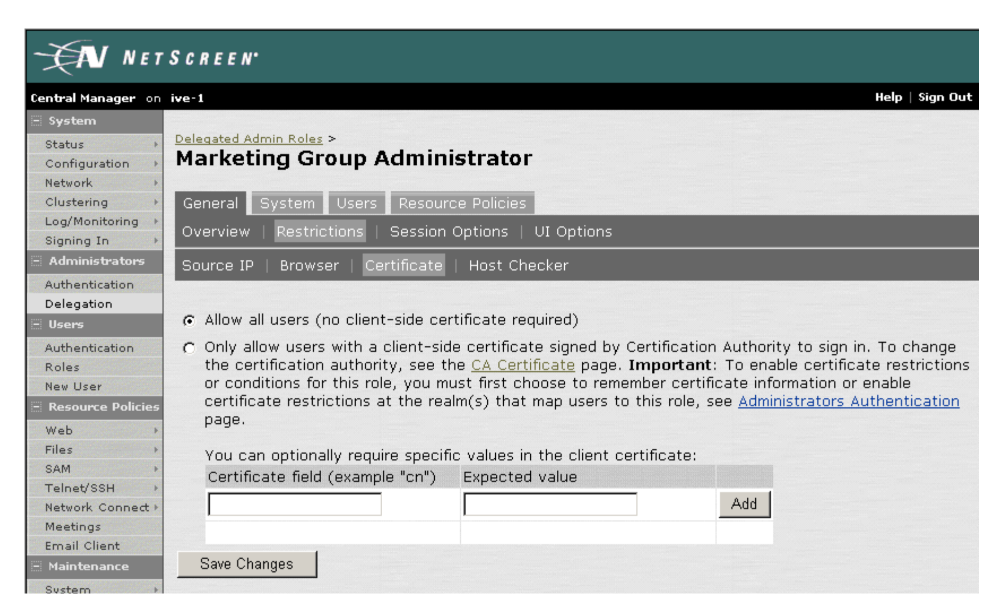


Abbildung 101: **Administrators > Delegation > [Rolle] > General > Restrictions > Certificate**

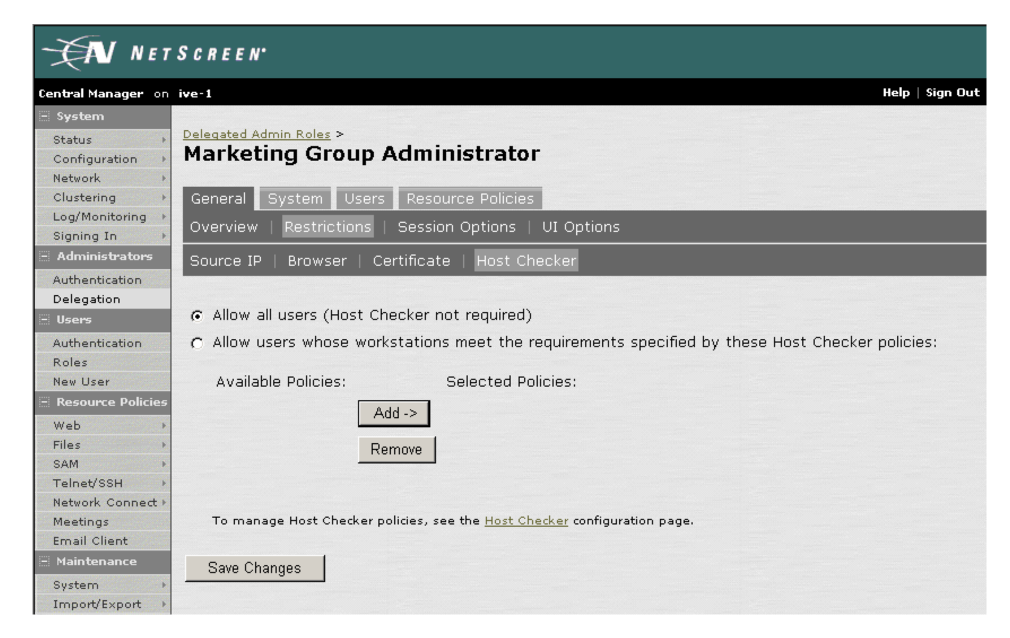


Abbildung 102: **Administrators > Delegation > [Rolle] > General > Restrictions > Host Checker**

Registerkarte „General > Session Options“

Auf der Registerkarte **General > Session Options** können Sie Sitzungszeitbegrenzungen und Roamingfunktionen angeben. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **Session Options**, um diese Einstellungen für die Rolle zu aktivieren.

☑ **Angeben von Sitzungszeit- und Roamingeinstellungen für Benutzer**

So geben Sie allgemeine Sitzungsoptionen an:

1. Klicken Sie in der Webkonsole auf **Administrators > Delegation >** ***Ausgewählte Rolle*** **> General > Session Options**.
2. Geben Sie unter **Session Lifetime** Werte für folgende Optionen an:
   - **Idle Timeout** – Geben Sie die Anzahl der Minuten an, die sich eine Administratorsitzung im Leerlauf befinden kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Leerlaufzeitbegrenzung für Sitzungen beträgt in der Standardeinstellung zehn Minuten, d. h., eine Administratorsitzung, die zehn Minuten lang inaktiv ist, wird vom IVE beendet, und das Ereignis wird im Systemprotokoll protokolliert (sofern Sie nicht die unten beschriebenen Warnungen bei Sitzungszeitüberschreitung aktivieren).
   - **Max. Session Length** – Geben Sie die Anzahl der Minuten an, die eine aktive Administratorsitzung geöffnet bleiben kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Standardzeitbegrenzung für eine Administratorsitzung beträgt sechzig Minuten. Nach dieser Zeitspanne beendet das IVE die Sitzung und protokolliert das Ereignis im Systemprotokoll.
3. Geben Sie unter **Roaming session** Folgendes an:
   - **Enabled** – Ermöglicht Roamingbenutzersitzungen für Benutzer, die dieser Gruppe zugeordnet sind. Eine Roamingbenutzersitzung funktioniert über Quell-IP-Adressen, wodurch sich mobile Administratoren (Benutzer von Laptops) mit dynamischen IP-Adressen von einem Standort aus im IVE anmelden können und ihre Arbeit von einem anderen Standort fortsetzen können. Einige Browser weisen jedoch eventuell Schwachstellen auf, über die durch bösartigen Code Benutzercookies gestohlen werden können. Ein böswilliger Benutzer kann dann ein gestohlenes IVE-Sitzungscookie verwenden, um sich im IVE anzumelden.

- **Limit to subnet** – Beschränkt die Roamingsitzung auf das lokale Subnetz, das im Feld **Netmask** angegeben ist. Administratoren können sich von einer IP-Adresse aus anmelden und ihre Sitzungen mit einer anderen IP-Adresse fortsetzen, sofern sich die neue IP-Adresse in demselben Subnetz befindet.
- **Disabled** – Deaktiviert Roamingsitzungen für Administratoren, die dieser Rolle zugeordnet sind. Administratoren, die sich von einer IP-Adresse aus anmelden, können eine aktive IVE-Sitzung nicht von einer anderen IP-Adresse aus fortsetzen. Administratorsitzungen sind an die ursprüngliche Quell-IP-Adresse gebunden.

4. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

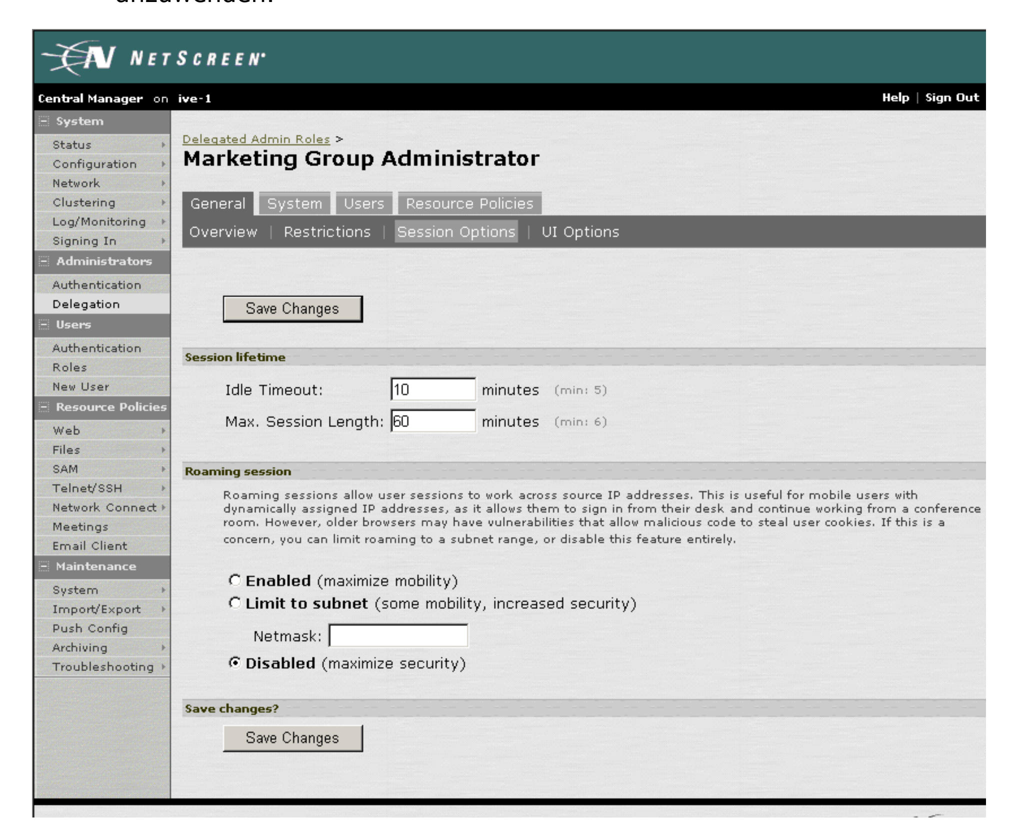


Abbildung 103: **Administrators > Delegation > [Rolle] > General > Session Options**

Registerkarte „General > UI Options“

Auf der Registerkarte **Administrators > Delegation > *Ausgewählte Rolle* > General > UI Options** können Sie benutzerdefinierte Einstellungen für die IVE-Willkommensseite für Administratoren angeben, die dieser Rolle zugeordnet sind. Die IVE-Willkommensseite (oder Startseite) ist die Weboberfläche, die authentifizierten IVE-Administratoren angezeigt wird. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **UI Options**, um diese Einstellungen für die Rolle zu aktivieren.

☑ **Anpassen der IVE-Willkommensseite für Benutzer mit Rollen**

So passen Sie die IVE-Willkommensseite für Benutzer mit Rollen an:

1. Wählen Sie in der Webkonsole **Administrators > Delegation > aus. *Ausgewählte Rolle* > General > UI Options**
2. Legen Sie im Abschnitt **Header** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Seitenkopf fest.
3. Wählen Sie im Abschnitt **Navigation Menus** aus, ob hierarchische Navigationsmenüs angezeigt werden sollen. ***Hierarchische Navigationsmenüs*** sind dynamische Menüs, die angezeigt werden, wenn Sie mit dem Mauszeiger auf eines der Menüs im linken Bereich von Webkonsole zeigen. Folgende Optionen stehen zur Verfügung:
   - **Auto-enabled** – Das IVE ermittelt, ob sich der Administrator von einer unterstützten Pattform aus angemeldet hat. Die hierarchischen Menüs werden entsprechend aktiviert bzw. deaktiviert.
   - **Enabled** – Das IVE aktiviert hierarchische Menüs unabhängig von Ihrer Plattform. Wenn sich ein Administrator über eine nicht unterstützte Plattform angemeldet hat, können die hierarchischen Menüs von ihm u. U. nicht verwendet werden, obwohl sie aktiviert sind.
   - **Disabled** – Das IVE deaktiviert hierarchische Menüs für alle Mitglieder der Rolle.

Hinweis:

- Informationen zu Umgebungen mit Unterstützung hierarchischer Menüs finden Sie auf der Juniper Networks-Supportsite im Dokument *IVE Supported Platforms*.
- Wenn Ihr System von Version 4.0 aktualisiert wurde, müssen Sie den Browsercache leeren oder einen neuen Browser öffnen, um die hierarchischen Menüs verwenden zu können.
- Hierarchische Menüs werden nur bei den Webkonsole-Untermenüs **System**, **Resource Policies** und **Maintenance** unterstützt.

4. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden.
5. Klicken Sie auf **Restore Factory Defaults**, um die Darstellung der Anmeldeseite, der IVE-Startseite für Administratoren und der Webkonsole zurückzusetzen.

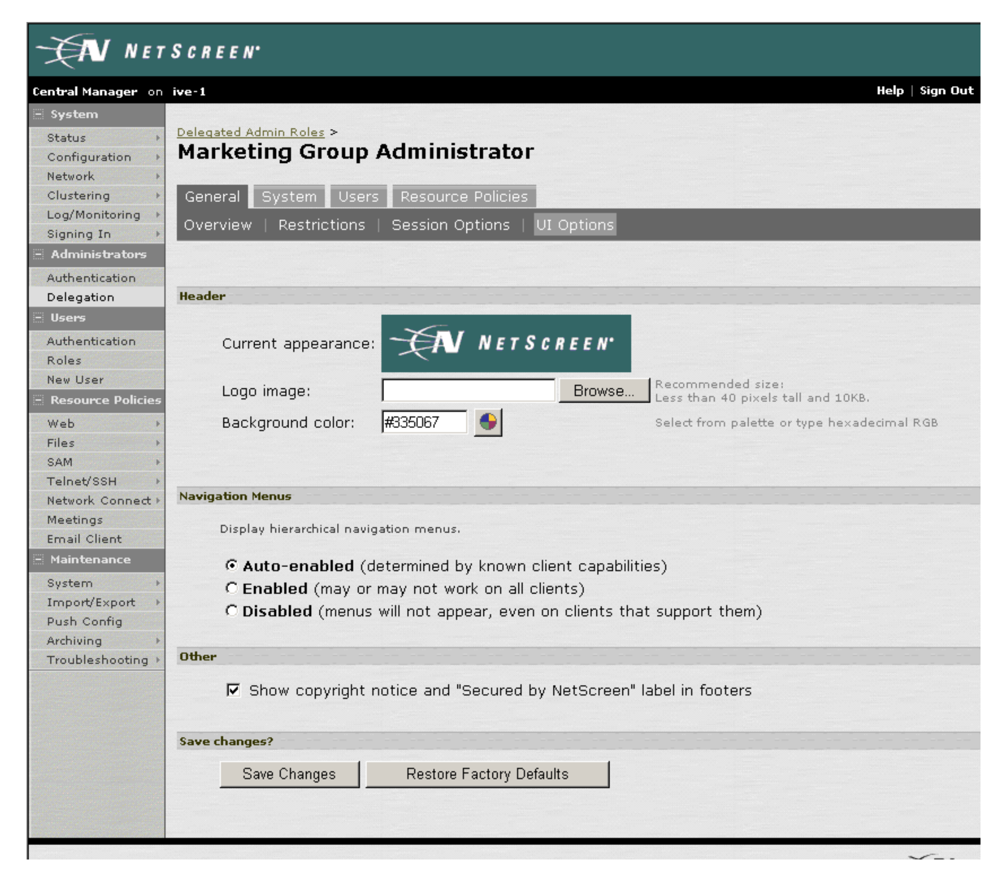


Abbildung 104: **Administrators > Delegation > [Rolle] > General > UI Options**

Registerkarte „System“

☑ Delegieren von Systemverwaltungsaufgaben

Auf dieser Registerkarte können Sie IVE-Systemverwaltungsaufgaben an verschiedene Administratorrollen delegieren. Beachten Sie beim Delegieren von Berechtigungen Folgendes:

- Alle Administratoren müssen unabhängig von der ausgewählten Berechtigungsebene über Lesezugriff (mindestens) auf die Webkonsole-Startseite (**System > Status > Overview**) verfügen.

- Delegierten Administratoren darf kein Schreibzugriff auf Seiten gewährt werden, auf denen Sie ihre eigenen Berechtigungen ändern können. Nur die systemintegrierten Administratorrollen (**.Administrators** und **.Read-Only Administrators**) dürfen auf diese Seiten zugreifen:
  - Administrators > Authentication
  - Administrators > Delegation
  - Users > New User
  - Maintenance > Import/Export (**.Read-Only Administrators** können Einstellungen auf dieser Seite exportieren, jedoch nicht importieren.)
  - Maintenance > Push Config
  - Maintenance > Archiving > Local Backups
- Das Delegieren des Zugriffs auf die Seite **Meeting Schedule** wird auf der Seite **Administrators > Delegation > [Rolle] > Resource Policies** über die Option **Meetings** gesteuert.

So legen Sie Administrationsberechtigungen für eine Administratorrolle fest:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Delegation** aus.
2. Wählen Sie die Administratorrolle aus, die Sie ändern möchten.
3. Klicken Sie auf die Registerkarte **System**.
4. Geben Sie die Zugriffsebene an, die der Administratorrolle für jede größere Gruppe von Webkonsole-Registerkarten (**System tasks**, **Signing In** und **Maintenance tasks**) gewährt werden soll, indem Sie eine der folgenden Optionen auswählen:
   - **Deny All** – Gibt an, dass Mitglieder der Administratorrolle keine Einstellungen in der Kategorie anzeigen oder ändern können.
   - **Read All** – Gibt an, dass Mitglieder der Administratorrolle Einstellungen in der Kategorie anzeigen, aber nicht ändern können.
   - **Read All** – Gibt an, dass Mitglieder der Administratorrolle alle Einstellungen in der Kategorie ändern können.
   - **Custom Settings** – Ermöglicht Ihnen die Auswahl von Administratorberechtigungen (**Deny**, **Read** oder **Write**) für die einzelnen Funktionen innerhalb der Kategorie.
5. Klicken Sie auf **Save Changes**.

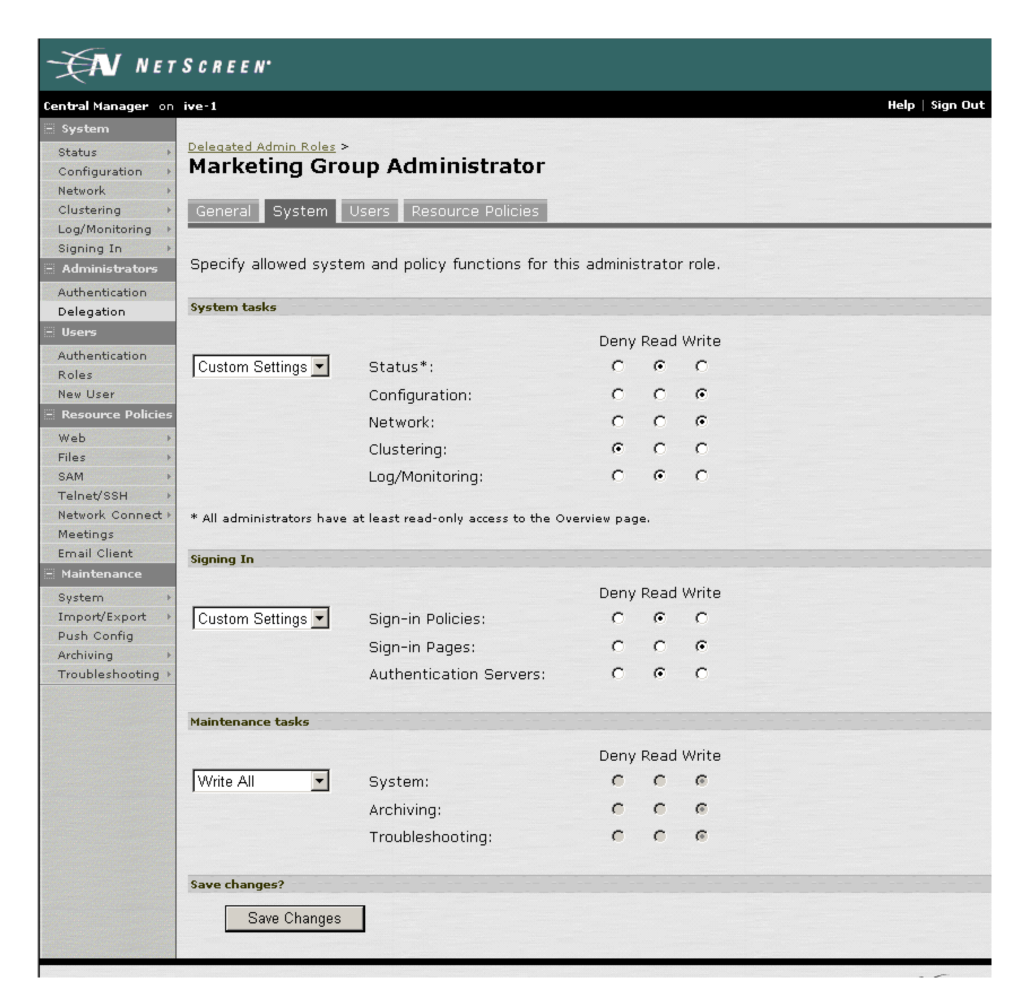


Abbildung 105: **Administrators > Delegation > [Rolle] > System**

Registerkarte „Users > Roles"

Auf dieser Registerkarte können Sie die Benutzerrollen angeben, die von einer Administratorrolle verwaltet werden können. Beachten Sie beim Delegieren von Rollenverwaltungsberechtigungen Folgendes:

- Delegierte Administratoren können nur Benutzerrollen verwalten.
- Delegierte Administratoren können keine neuen Benutzerrollen erstellen und können vorhandene Rollen nicht kopieren oder löschen.
- Wenn Sie dem delegierten Administrator für alle Funktionen innerhalb einer Benutzerrolle Lese- oder Schreibzugriff gewähren, gestattet ihm das IVE auch Lesezugriff auf die Seite **Users > Role > [Rolle] > General > Overview** für diese Rolle.
- Wenn Sie einem delegierten Administrator über die Seite **Administrators > Delegation > [Administratorrolle] > System** Schreibzugriff auf eine Ressourcenrichtlinie erteilen, kann er eine Ressourcenrichtlinie erstellen, die auf alle Benutzerrollen anwendbar ist, auch wenn er nicht über Lesezugriff auf diese Rolle verfügt.

☑ **Delegieren von Benutzerrollenverwaltung an eine Administratorrolle**

So definieren Sie Rollenverwaltungsberechtigungen für eine Administratorrolle:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Delegation** aus.
2. Wählen Sie die Administratorrolle aus, die Sie ändern möchten.
3. Klicken Sie auf die Registerkarte **Users > Roles**.
4. Geben Sie unter **Delegated user roles** an, ob der Administrator alle Rollen oder nur ausgewählte Rollen verwalten darf. Wenn der Administratorrolle nur das Verwalten ausgewählter Benutzerrollen gestattet werden soll, wählen Sie die entsprechenden Rollen in der Liste **Available Role** aus und klicken auf **Add**.

5. Geben Sie an, welche Benutzerrollenseiten vom delegierten Administrator verwaltet werden können, indem Sie eine der folgenden Optionen auswählen:
    - **Write All** – Gibt an, dass Mitglieder der Administratorrolle alle Benutzerrollenseiten ändern können.
    - **Custom Settings** – Ermöglicht Ihnen das Auswählen von Administratorberechtigungen (**Deny**, **Read** oder **Write**) für die einzelnen Benutzerrollenseiten.
6. Wählen Sie unter **Delegate as read-only roles** die Benutzerrollen aus, die der Administrator anzeigen, jedoch nicht verwalten darf.

    Hinweis: Wenn Sie für eine Funktion sowohl Schreib- als auch Lesezugriff angeben, gewährt das IVE hierfür den umfassendsten Zugriff. Wenn Sie z. B. unter **Delegated user roles** die Option **Administrators can manage ALL roles** auswählen und anschließend im Abschnitt **Delegate as read-only roles** die Rolle „Users“ auswählen, gewährt das IVE der delegierten Administratorrolle umfassende Verwaltungsberechtigungen für die Rolle „Users“.

7. Klicken Sie auf **Save Changes**.

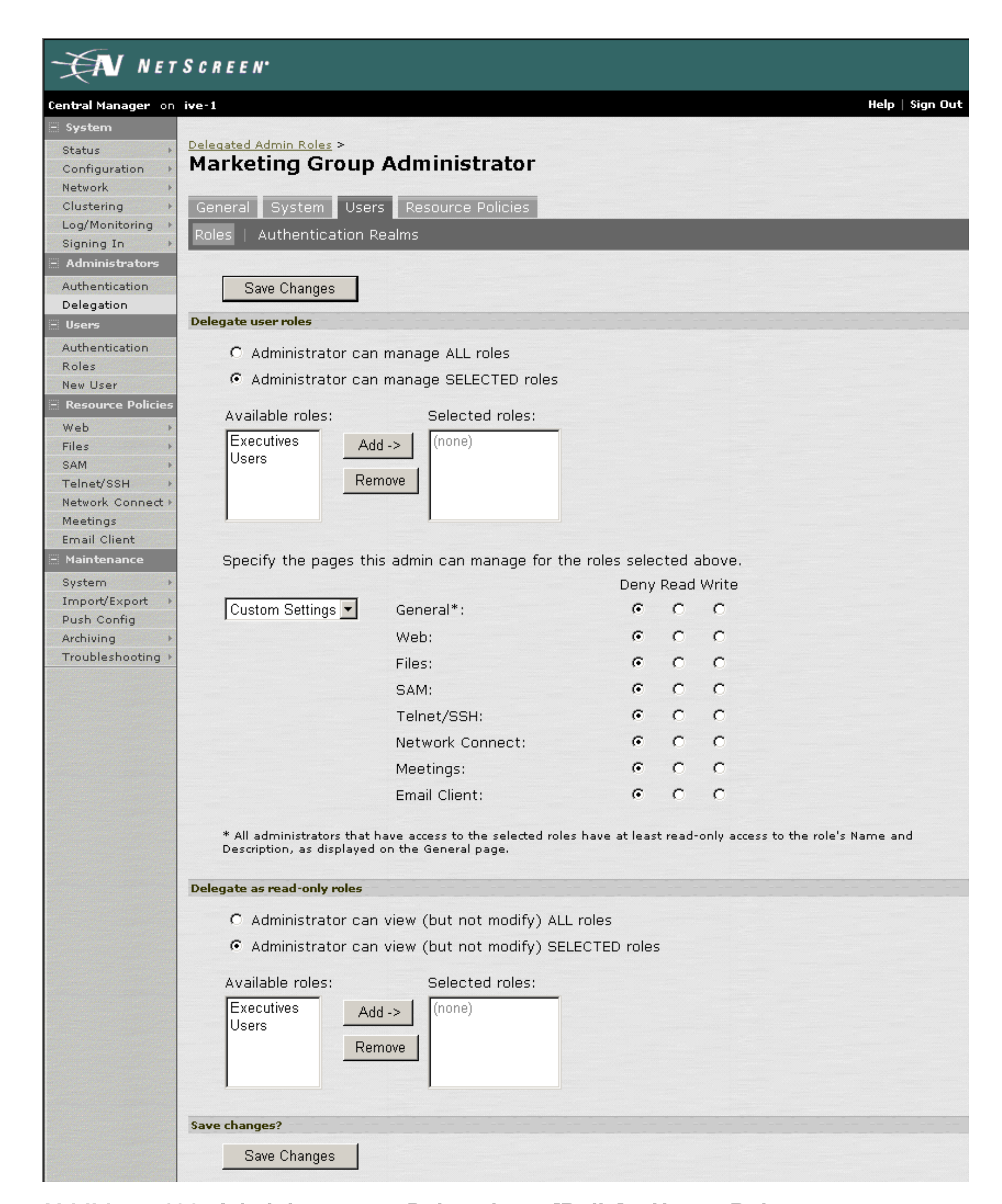


Abbildung 106: **Administrators > Delegation > [Rolle] > User > Roles**

Registerkarte „Users > Authentication Realms“

Auf dieser Registerkarte können Sie die Benutzerauthentifizierungsbereiche angeben, die von der Administratorrolle verwaltet werden können. Beachten Sie beim Delegieren von Bereichsverwaltungsberechtigungen Folgendes:

- Delegierte Administratoren können nur Benutzerbereiche verwalten.
- Delegierte Administratoren können keine neuen Benutzerbereiche erstellen und vorhandene Bereiche nicht kopieren oder löschen.
- Wenn Sie dem delegierten Administrator Schreib- oder Lesezugriff für Benutzerbereichsseiten gewähren, gestattet ihm das IVE auch Lesezugriff auf die Seite **User > Authentication > [Bereich] > General** für diese Rolle.

☑ **Delegieren der Benutzerbereichsverwaltung**

So definieren Sie Bereichsverwaltungsberechtigungen für eine Administratorrolle:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Delegation** aus.
2. Wählen Sie die Administratorrolle aus, die Sie ändern möchten.
3. Klicken Sie auf die Registerkarte **Users > Authentication Realms**.
4. Geben Sie unter **Delegated user realms** an, ob der Administrator alle oder nur ausgewählte Benutzerauthentifizierungsbereiche verwalten kann. Wenn der Administratorrolle nur das Verwalten ausgewählter Bereiche gestattet werden soll, wählen Sie die entsprechenden Bereiche in der Liste **Available Role** aus und klicken auf **Add**.
5. Geben Sie an, welche Seiten von Benutzerauthentifizierungsbereichen vom delegierten Administrator verwaltet werden können, indem Sie eine der folgenden Optionen auswählen:
   - **Write All** – Gibt an, dass Mitglieder der Administratorrolle alle Seiten von Benutzerauthentifizierungsbereichen ändern können.
   - **Custom Settings** – Ermöglicht Ihnen das Auswählen von Administratorberechtigungen (**Deny**, **Read** oder **Write**) für die einzelnen Seiten von Benutzerauthentifizierungsbereichen.

6. Wählen Sie unter **Delegate as read-only realms** die Benutzerauthentifizierungsbereiche aus, die der Administrator anzeigen, jedoch nicht verwalten darf.

Hinweis: Wenn Sie für eine Authentifizierungsbereichsseite sowohl Schreib- als auch Lesezugriff angeben, gewährt das IVE hierfür den umfassendsten Zugriff. Wenn Sie z. B. unter **Delegated user realms** die Option **Administrators can manage ALL realms** auswählen und anschließend im Abschnitt **Delegate as read-only realms** die Rolle „Users" auswählen, gewährt das IVE der delegierten Administratorrolle umfassende Verwaltungsberechtigungen für den Bereich „Users".

---

7. Klicken Sie auf **Save Changes**.

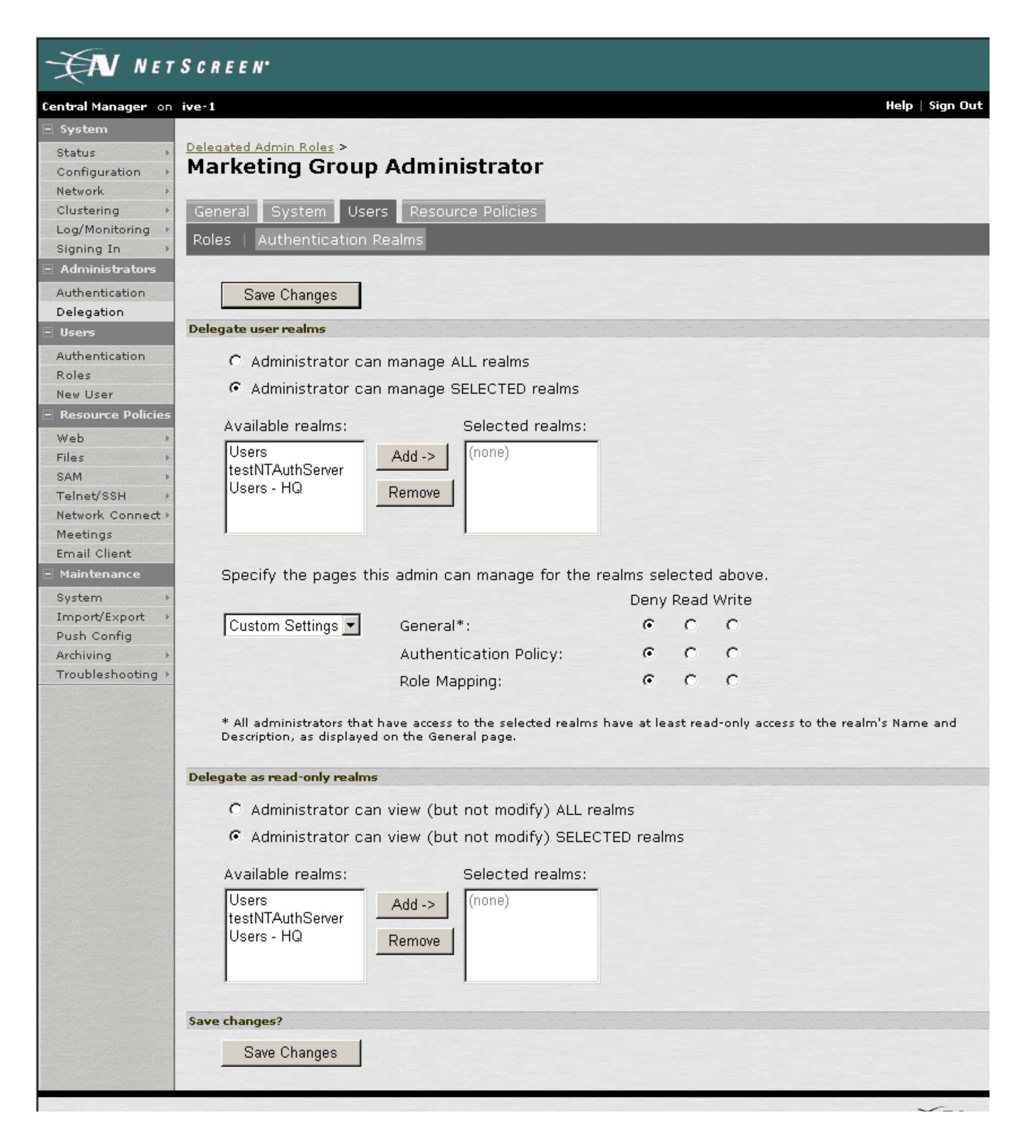


Abbildung 107: **Administrators > Delegation > [Rolle] > User > Authentication Realms**

Registerkarte „Resource Policies“

Auf dieser Registerkarte können Sie die Benutzerressourcenrichtlinien angeben, die von einer Administratorrolle verwaltet werden können. Beachten Sie beim Delegieren von Verwaltungsberechtigungen für Ressourcenrichtlinien, dass die folgenden Merkmale von Ressourcenrichtlinien von delegierten Administratoren nicht geändert werden können:

- die Ressource selbst (d. h. die IP-Adresse oder der Hostname)
- die Reihenfolge, in der die Ressourcenrichtlinien vom IVE ausgewertet werden

☑ Delegieren von Administratorberechtigungen für Ressourcenrichtlinien

So delegieren Sie Administratorberechtigungen für Ressourcenrichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Delegation** aus.
2. Wählen Sie die Administratorrolle aus, die Sie ändern möchten.
3. Klicken Sie auf die Registerkarte **Resource Policies**.
4. Geben Sie die Zugriffsebene an, die der Administratorrolle für jedes **Resource Policies**-Untermenü gewährt werden soll, indem Sie eine der folgenden Optionen auswählen:
   - **Deny All** – Gibt an, dass Mitglieder der Administratorrolle keine Ressourcenrichtlinien anzeigen oder ändern können.
   - **Read All** – Gibt an, dass Mitglieder der Administratorrolle alle Ressourcenrichtlinien anzeigen, aber nicht ändern können.
   - **Write All** – Gibt an, dass Mitglieder der Administratorrolle alle Ressourcenrichtlinien ändern können.
   - **Custom Settings** – Ermöglicht Ihnen das Auswählen von Administratorberechtigungen (**Deny**, **Read** oder **Write**) für alle Ressourcenrichtlinientypen bzw. für einzelne Ressourcenrichtlinien.
5. Wenn Sie benutzerdefinierte Zugriffsebenen für eine einzelne Richtlinie festlegen möchten, gehen Sie folgendermaßen vor:
   1. Wählen Sie **Custom Settings** aus (siehe oben).
   2. Klicken Sie auf die Verknüpfung **Additional Access Policies** neben der entsprechenden Kategorie. (Wenn Sie z. B. den Zugriff auf eine Ressourcenrichtlinie steuern möchten, durch die der Zugriff auf www.google.com geregelt wird, klicken Sie auf die Verknüpfung Additional Access Policies neben **Web**.)

3 Wählen Sie die Zugriffsebene für die Richtlinie aus (**Deny**, **Read** oder **Write**).

4 Wählen Sie unter **Access Policies** die Ressourcenrichtlinie aus, für die eine benutzerdefinierte Zugriffsebene bereitgestellt werden soll, und klicken Sie auf **Add**.

6. Klicken Sie auf **Save Changes**.

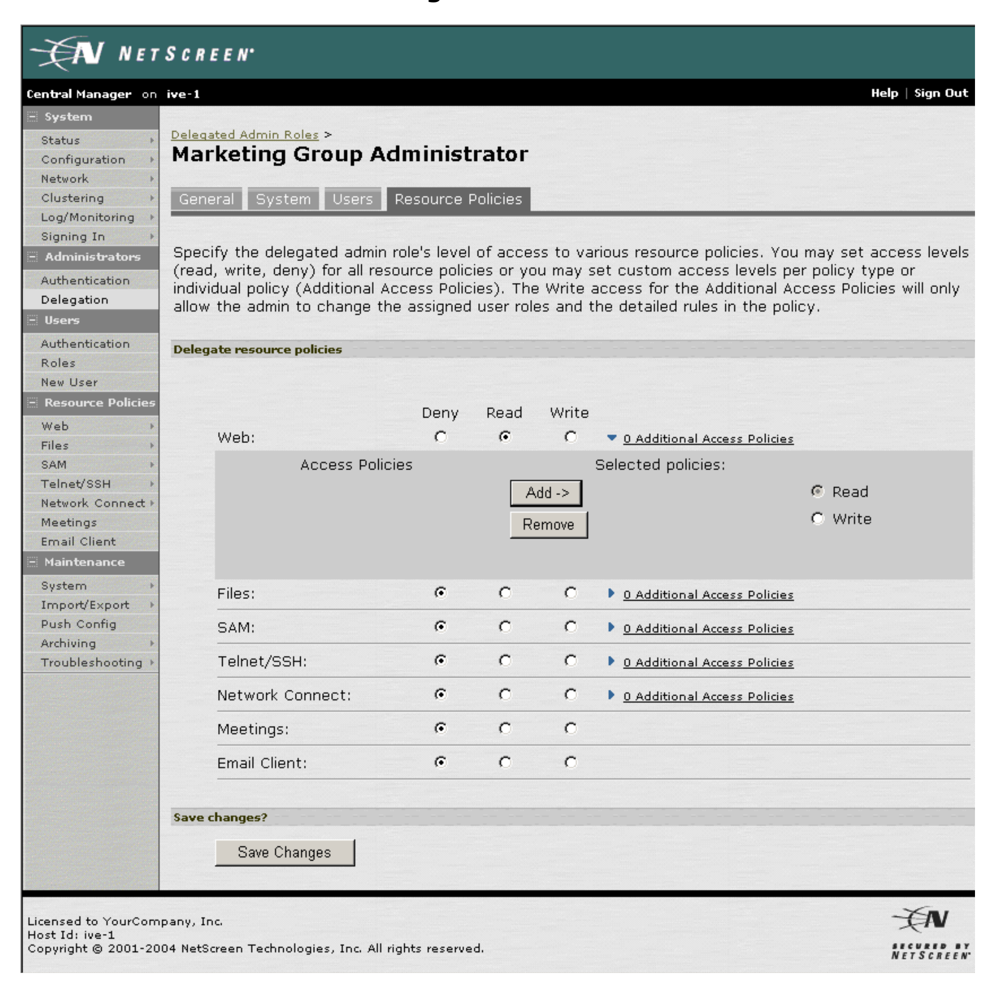


Abbildung 108: **Administrators > Delegation > [Rolle] > Resource Policies**

Konfigurieren eines Authentifizierungsbereichs

Über die Menüs **Administrators > Authentication** und **Users > Authentication** können Benutzer auf die entsprechenden Seiten für **Authentication Realms** zugreifen. Auf diesen Seiten können Sie Authentifizierungsbereiche im System erstellen und verwalten.

Die Seite **Authentication Realms** enthält die folgenden Registerkarten:

Auf den Registerkarten der Seite **Authentication Realms** können Sie Folgendes durchführen:

Registerkarte „General“

Auf der Registerkarte **General** können Sie einen Authentifizierungsbereich erstellen. Weitere Informationen zu Bereichen finden Sie unter „Authentifizierungsbereiche – Übersicht“ auf Seite 35.

☑ Erstellen eines Authentifizierungsbereichs

So erstellen Sie einen Authentifizierungsbereich:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Authentication** oder **Users > Authentication** aus.
2. Klicken Sie auf der entsprechenden Seite **Authentication Realms** auf **New Realm**.
3. Verfahren Sie auf der Seite **New Realm** folgendermaßen:
   1 Geben Sie eine Bezeichnung für diesen Bereich ein.
   2 Geben Sie eine Beschreibung für den Bereich ein. (Dies ist optional.)

3 Aktivieren Sie **When editing, start on the Role Mapping page**, wenn die Registerkarte **Role Mapping** beim Öffnen des Bereichs zur Bearbeitung aktiviert sein soll.

4. Legen Sie unter **Servers** Folgendes fest:
   - Einen Authentifizierungsserver, der zum Authentifizieren von Benutzern verwendet werden soll, die sich bei diesem Bereich anmelden.
   - Einen Verzeichnis-/Attributserver zum Abrufen von Benutzerattributen und Gruppeninformationen für Rollenzuordnungsregeln und Ressourcenrichtlinien. (Dies ist optional.)
5. Klicken Sie auf **Save Changes**, um den Bereich auf dem IVE zu erstellen. Die Registerkarten **General**, **Authentication Policy** und **Role Mapping** für den Authentifizierungsbereich werden angezeigt.
6. Führen Sie die nächsten Konfigurationsschritte aus:
   1 Konfigurieren Sie mindestens eine Rollenzuordnungsregel. (Seite 382)
   2 Konfigurieren Sie eine Authentifizierungsrichtlinie für den Bereich. (Seite 381)

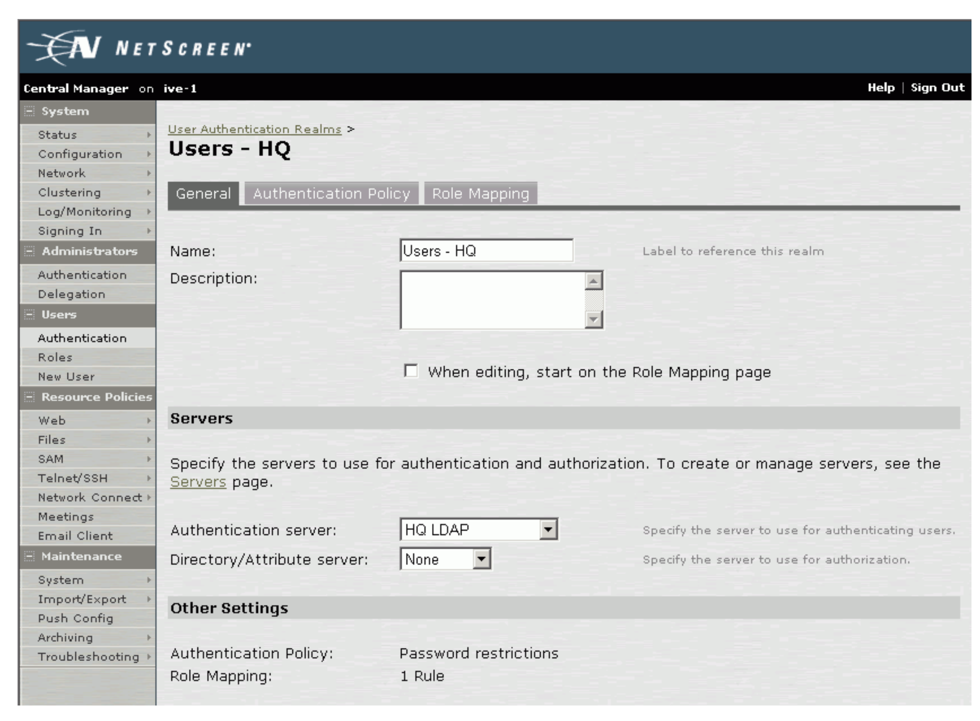


Abbildung 109: **Users | Administrators > Authentication >** ***Bereichsname*** **> General**

Registerkarte „Authentication Policy“

Auf der Registerkarte **Authentication Policy** können Sie eine Richtlinie für einen Authentifizierungsbereich erstellen. Weitere Informationen zu Bereichen finden Sie unter „Authentifizierungsbereiche – Übersicht“ auf Seite 35.

☑ Angeben einer Richtlinie für einen Authentifizierungsbereich

So geben Sie eine Richtlinie für einen Authentifizierungsbereich an:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Authentication** oder **Users > Authentication** aus.
2. Wählen Sie auf der entsprechenden Seite **Authentication Realms** einen Bereich aus, und klicken Sie dann auf die Registerkarte **Authentication Policy**.
3. Konfigurieren Sie auf der Seite **Authentication Policy** mindestens eine der folgenden Zugriffsverwaltungsoptionen:
   - Quell-IP (Seite 584)
   - Browser (Seite 585)
   - Zertifikat (Seite 587)
   - Kennwort (Seite 589)
   - Hostprüfung (Seite 590)
   - Cachebereinigung[1] (Seite 591)
   - Begrenzungen (Seite 381)

Begrenzungen für gleichzeitig angemeldete Benutzer

Neben den Zugriffsverwaltungsoptionen, die Sie für eine Authentifizierungsrichtlinie festlegen können, können Sie auch die Höchstanzahl gleichzeitig angemeldeter Benutzer festlegen. Konfigurieren Sie diese Einstellung hier:

- Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Limits
- Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Limits

1. In Administratorbereichen nicht verfügbar.

Nur wenn ein Benutzer, der auf einer der Anmeldeseiten dieses Bereichs einen URL eingibt, alle Benutzeranforderungen hinsichtlich Zugriffsverwaltung und gleichzeitig angemeldeter Benutzer erfüllen, die für die Authentifizierungsrichtlinie festgelegt sind, wird vom IVE eine Anmeldeseite geöffnet.

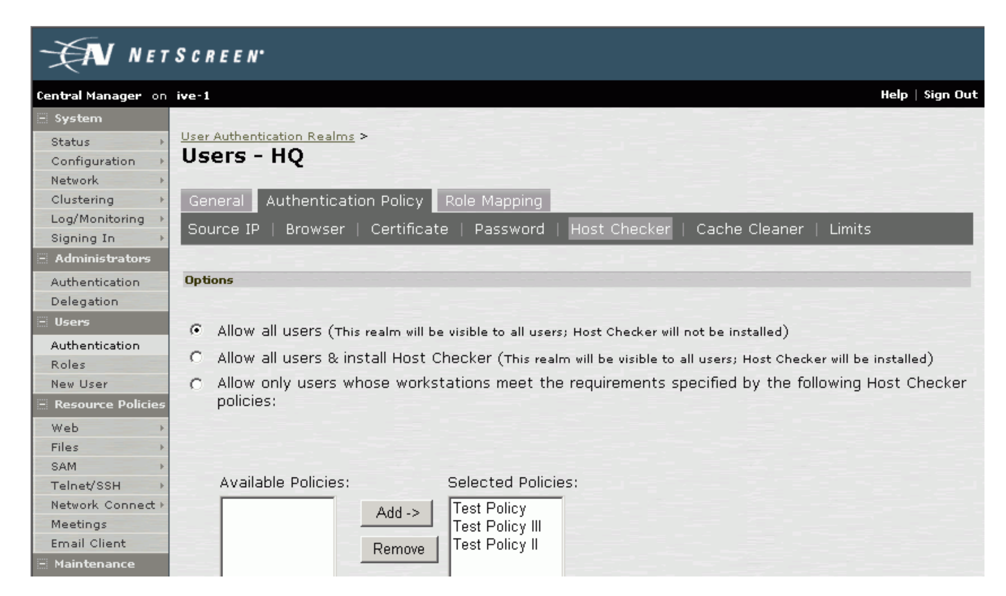


Abbildung 110: **Users | Administrators > Authentication > *Bereichsname* > Authentication Policy**

Registerkarte „Role Mapping“

Auf der Registerkarte **Role Mapping** können Sie Rollenzuordnungsregeln für einen Authentifizierungsbereich festlegen. Entsprechende Informationen finden Sie auf folgenden Seiten:

- Bereiche siehe „Authentifizierungsbereiche – Übersicht“ auf Seite 35.
- Rollen siehe „Benutzerrollen – Übersicht“ auf Seite 55.

☑ Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich

Zum Erstellen einer neuen Regel, die LDAP-Benutzerattribute, LDAP-Gruppeninformationen oder benutzerdefinierte Ausdrücke verwendet, müssen Sie den Serverkatalog verwenden. Informationen zu diesem Katalog finden Sie unter „Verwenden des Serverkatalogs“ auf Seite 385.

So geben Sie Rollenzuordnungsregeln für einen Authentifizierungsbereich an:

1. Wählen Sie in der Webkonsole die Optionen **Administrators > Authentication** oder **Users > Authentication** aus.
2. Wählen Sie auf der entsprechenden Seite **Authentication Realms** einen Bereich aus, und klicken Sie dann auf die Registerkarte **Role Mapping**.
3. Klicken Sie auf **New Rule**, um auf die Seite **Role Mapping Rule** zuzugreifen. Diese Seite stellt einen integrierten Editor für die Definition von Regeln bereit.
4. Wählen Sie in der Liste **Rule based on** eines der folgenden Elemente aus:
   - **Username**

     Username ist der IVE-Benutzername, der auf der Anmeldeseite eingegeben wird. Wählen Sie diese Option aus, wenn Benutzer anhand ihrer IVE-Benutzernamen zu Rollen zugeordnet werden sollen. Dieser Regeltyp ist für alle Bereiche verfügbar.
   - **User attribute**

     Userattribute ist ein Benutzerattribut, das entweder aus einem RADIUS- oder einem LDAP-Server stammt. Wählen Sie diese Option aus, wenn Benutzer anhand eines Attributs vom entsprechenden Server zu Rollen zugeordnet werden sollen. Dieser Regeltyp steht nur für Bereiche zur Verfügung, die einen RADIUS-Server als Authentifzierungsserver oder einen LDAP-Server als Authentifizierungs- bzw. Verzeichnisserver verwenden.
   - **Certificate** oder **Certificate attribute**

     Certificate oder *Certificate attribute* ist ein Attribut, das vom clientseitigen Zertifikat des Benutzers unterstützt wird. Wählen Sie diese Option aus, wenn Benutzer anhand ihrer Zertifikatsattribute zu Rollen zugeordnet werden sollen. Die Option *Certificate* ist für alle Bereiche verfügbar, während die Option *Certificate attribute* nur für Bereiche verfügbar ist, die einen LDAP-Authentifizierungs- oder Verzeichnisserver verwenden.
   - **Group membership**

     Group membership ist eine Angabe zur Gruppe von einem LDAP-Server oder systemeigenen Active Directory-Server, die Sie der Registerkarte **Groups** des Serverkatalogs hinzufügen. Wählen Sie diese Option aus, wenn Benutzer anhand der LDAP- bzw. Active Directory-Gruppeninformationen Rollen zugeordnet werden sollen. Dieser Regeltyp steht nur für Bereiche zur Verfügung, die einen LDAP-Server als Authentifizierungs- oder Verzeichnisserver verwenden oder die einen Active Directory-Server für die Authentifizierung verwenden. (Beachten Sie, dass ein Active Directory-Server nicht als Autorisierungsserver für einen Bereich angegeben werden kann.)

- **Custom Expressions**

  Custom Expressions sind benutzerdefinierte Ausdrücke, die Sie im Serverkatalog definieren. Wählen Sie diese Option aus, wenn Benutzer anhand benutzerdefinierter Ausdrücke zu Rollen zugeordnet werden sollen. Dieser Regeltyp ist für alle Bereiche verfügbar.

5. Geben Sie unter **Rule** die auszuwertende Bedingung an, die dem ausgewählten Regeltyp entspricht und folgende Punkte umfasst:
   1. Angeben von mindestens einem Benutzernamen, RADIUS- oder LDAP-Benutzerattribut, Zertifikatsattribut, einer LDAP-Gruppe oder einem benutzerdefinierten Ausdruck.
   2. Angeben der Wertentsprechungen. Dies kann auch eine Liste von IVE-Benutzernamen, Benutzerattributswerten von einem RADIUS- oder LDAP-Server, clientseitigen Zertifikatswerten (statische oder LDAP-Attributwerte), LDAP-Gruppen oder benutzerdefinierten Ausdrücken umfassen.
6. Nehmen Sie unter **...then assign these roles** folgende Eingaben vor:
   1. Geben Sie die Rollen an, die Sie dem authentifizierten Benutzer zuordnen möchten, indem Sie Rollen zur Liste **Selected Roles** hinzufügen.
   2. Aktivieren Sie die Option **Stop processing rules when this rule matches**, wenn das IVE die Auswertung der Rollenzuordnungsregeln anhalten soll, wenn der Benutzer die für diese Regel angegebenen Bedingungen erfüllt.
7. Klicken Sie auf **Save Changes**, um die Regel auf der Registerkarte **Role Mapping** zu erstellen. Gehen Sie nach dem Abschluss der Regelerstellung folgendermaßen vor:
   - Bringen Sie die Regeln unbedingt in die Reihenfolge, in der das IVE diese auswerten soll. Diese ist besonders dann wichtig, wenn die Verarbeitung der Rollenzuordnungsregeln bei einer Übereinstimmung angehalten werden soll.
   - Geben Sie an, ob die Einstellungen für alle zugeordneten Rollen zusammengeführt werden sollen. Weitere Informationen finden Sie unter „Richtlinien für permissive Zusammenführungen" auf Seite 58.

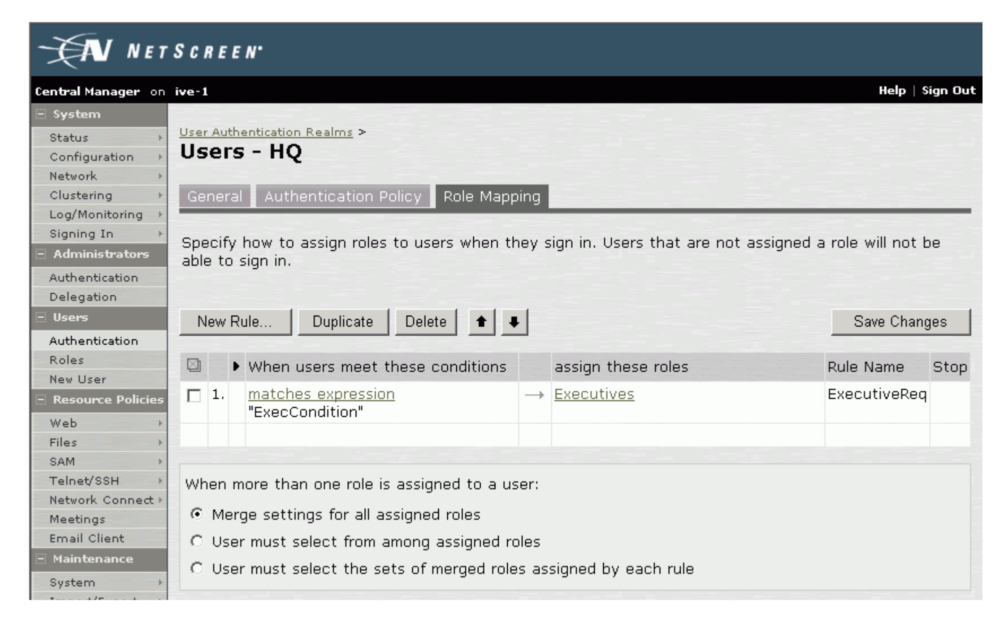


Abbildung 111: **Users | Administrators > Authentication > *Bereichsname* > Role Mapping**

☑ Verwenden des Serverkatalogs

Der ***Server Catalog*** ist ein sekundäres Fenster, in dem Sie Zusatzinformationen angeben können, die das IVE für die Zuordnung von Benutzern zu Rollen verwendet, darunter:

- **Attributes**

  Auf der Registerkarte **Server Catalog Attributes** wird eine Liste von allgemeinen LDAP-Attributen angezeigt, z. B. `cn`, `uid`, `uniquemember` und `memberof`. Diese Registerkarte kann nur beim Zugriff auf den Serverkatalog eines LDAP-Servers aufgerufen werden. Auf dieser Registerkarte können Sie die Attribute eines LDAP-Servers verwalten, indem Sie seinem IVE-Serverkatalog benutzerdefinierte Werte hinzufügen oder Werte aus diesem löschen. Beachten Sie, dass das IVE eine lokale Kopie der LDAP-Serverwerte aufbewahrt. Attribute werden dem Wörterbuch weder hinzugefügt noch aus diesem gelöscht.

- **Groups**

  Über die Registerkarte **Server Catalog Groups** können Gruppeninformationen einfach von einem LDAP-Server abgefragt und dem Serverkatalog eines IVE-Servers hinzugefügt werden. Sie geben den BaseDN der Gruppen und ggf. einen Filter an, um die Suche zu starten. Wenn Ihnen der genaue Container der Gruppen nicht bekannt ist, können Sie den Domänenstamm als BaseDN festlegen, z. B. `dc=juniper, dc=com`.

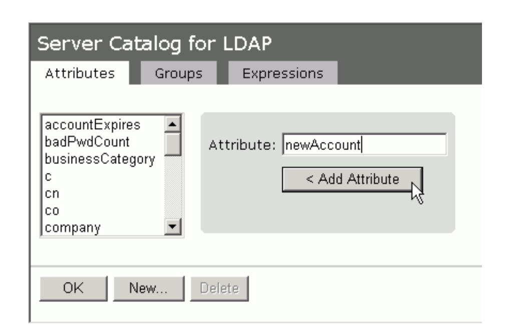
Die Suchseite gibt eine Gruppenliste vom Server zurück, aus der Sie Gruppen auswählen können, die in die Liste **Groups** eingegeben werden.

Hinweis: Der auf der Konfigurationsseite des LDAP-Servers unter „Finding user entries“ angegebene BaseDN-Wert ist der Standard-BaseDN-Wert. Der Filterwert ist standardmäßig auf (cn=*) gesetzt.

Sie können Gruppen auch auf der Registerkarte **Groups** angeben. Sie müssen den FQDN (Fully Qualified Distinguished Name) einer Gruppe angeben, z. B. cn=Manager, ou=Zentrale, ou=Juniper, o=com, c=DE, können dieser Gruppe jedoch eine Bezeichnung zuordnen, die in der Liste **Groups** angezeigt wird. Beachten Sie, dass diese Registerkarte nur beim Zugriff auf den Serverkatalog eines LDAP-Servers aufgerufen werden kann.

- **Expressions**

  Auf der Registerkarte **Server Catalog Expressions** können Sie benutzerdefinierte Ausdrücke für die Rollenzuordnungsregel schreiben. Weitere Informationen zu benutzerdefinierten Ausdrücken finden Sie in Anhang D.: auf Seite 595.



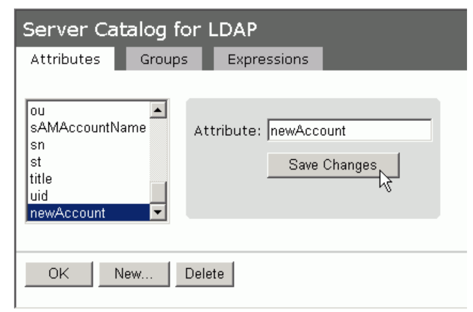


Abbildung 112: **Registerkarte „Server Catalog > Attributes“ – Hinzufügen eines Attributs**

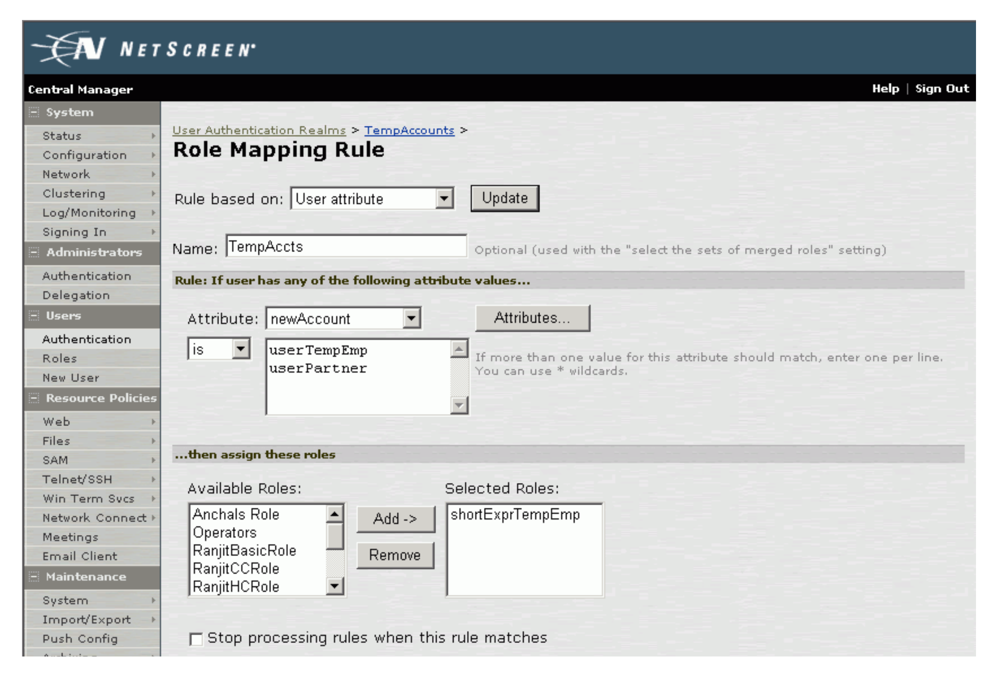
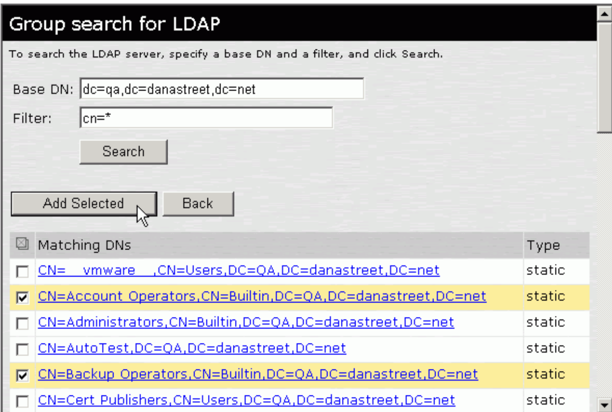


Abbildung 113: Das im Serverkatalog hinzugefügte Attribut steht für die Rollenzuordnungsregel zur Verfügung





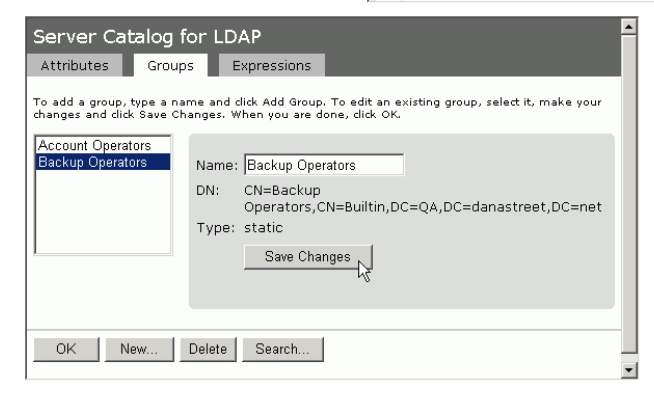


Abbildung 114: **Registerkarte „Server Catalog > Groups" – Hinzufügen von LDAP-Gruppen**

Server Catalog for Win2K QA Active Directory Server
Attributes
Groups
Expressions
To add a group, type a name and click Add Group. To edit an existing group, select it, make your changes and click Save Changes. When you are done, click OK.
(none)
Name:
Group:
Enter group as DOMAIN/GroupName
< Add Group
OK
New...
Delete
Search...



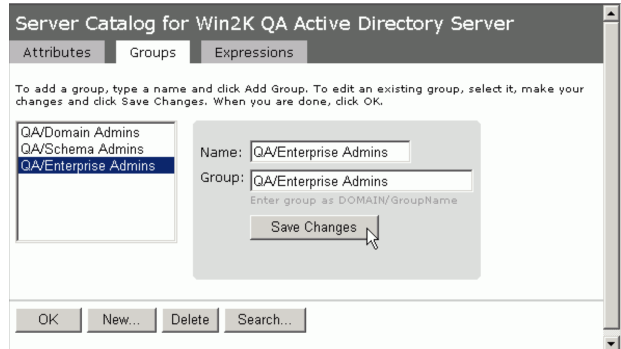


Abbildung 115: **Registerkarte „Server Catalog > Groups" – Hinzufügen von Active Directory-Gruppen**

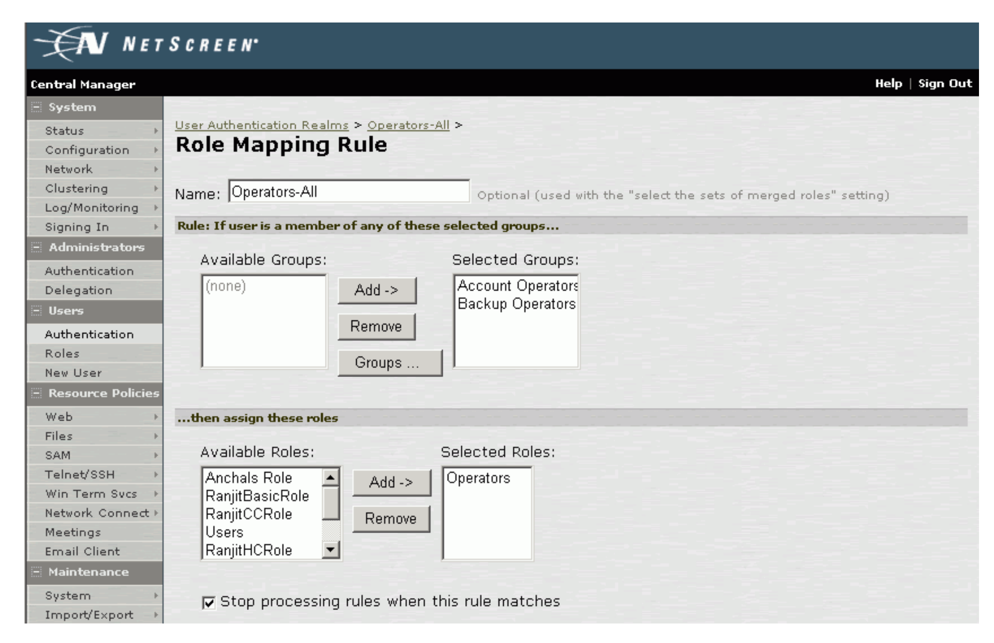


Abbildung 116: Die im Serverkatalog hinzugefügten LDAP-Gruppen stehen für die Rollenzuordnungsregel zur Verfügung

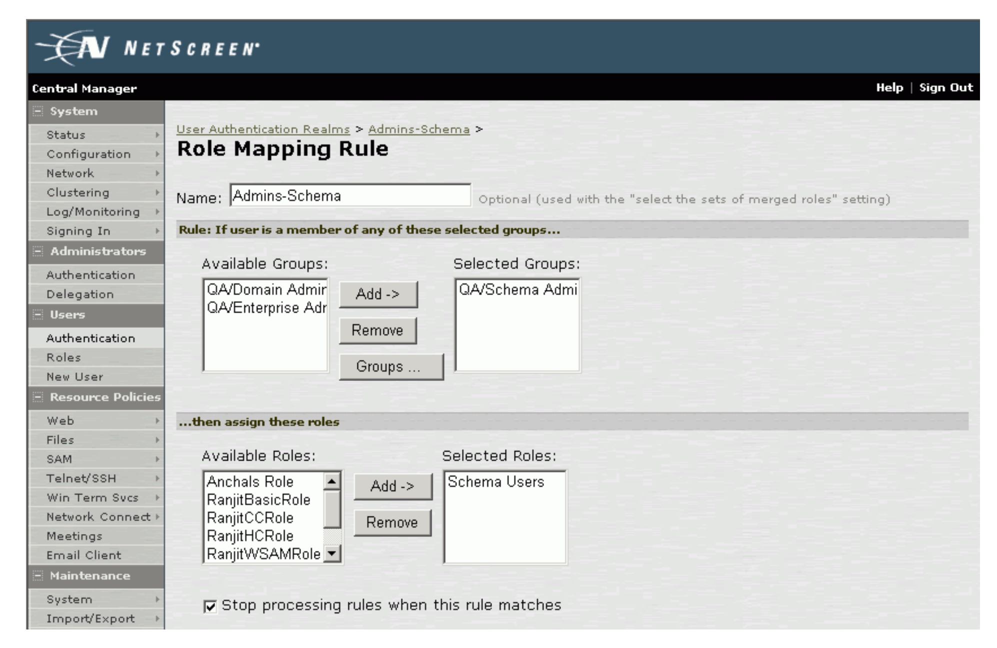


Abbildung 117: Die im Serverkatalog hinzugefügten AD-Gruppen stehen für die Rollenzuordnungsregel zur Verfügung

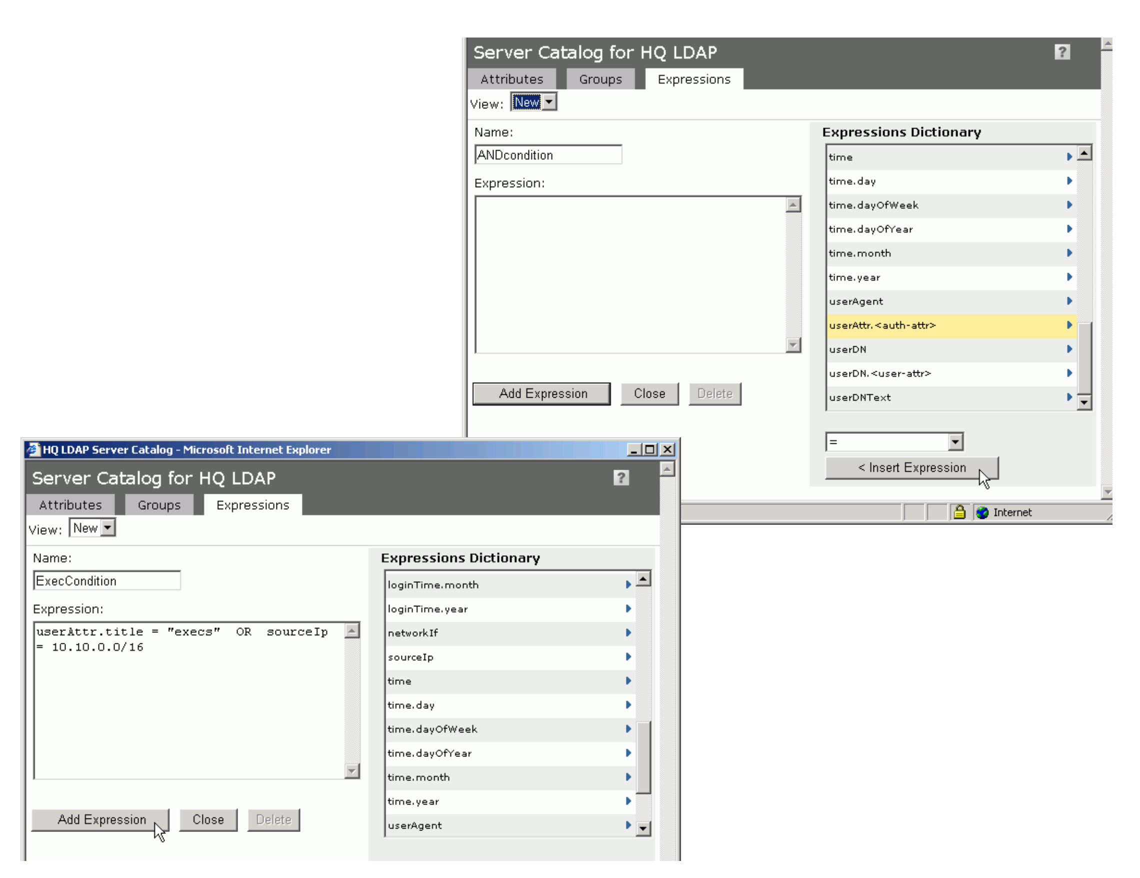


Abbildung 118: Registerkarte „Server Catalog > Expressions“ – Hinzufügen eines benutzerdefinierten Ausdrucks

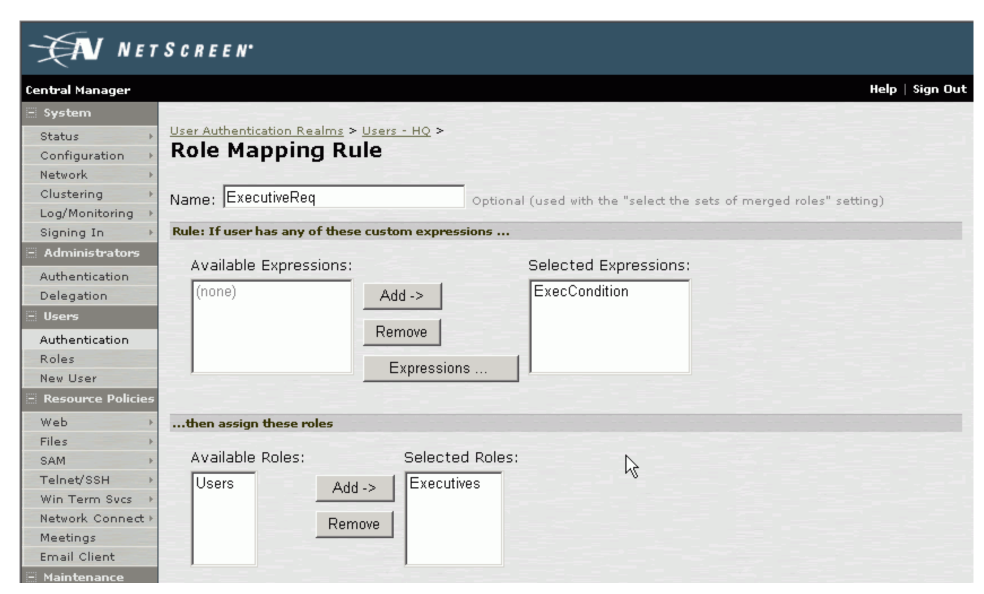


Abbildung 119: **Der im Serverkatalog hinzugefügte benutzerdefinierte Ausdruck steht für die Rollenzuordnungsregel zu Verfügung**

Konfigurieren der Seite „Roles“

Das Menü **Users > Roles** ist mit den Seiten **Roles** für Benutzer verknüpft. Auf dieser Seite können Sie Benutzerrollen im System erstellen und verwalten. Klicken Sie zum Erstellen einer Rolle auf **New Role**, und geben Sie dann einen Namen sowie bei Bedarf eine Beschreibung ein. Dieser Name wird auf der Seite **Roles** in der Liste **Roles** angezeigt. Klicken Sie auf den Namen der Rolle, um auf den Registerkarten für Rollen mit der Konfiguration zu beginnen.

Die Seite **Users > Roles** enthält die folgenden Registerkarten:

Auf den Registerkarten der Seite **Users > Roles** können Sie Folgendes durchführen:

Registerkarte „General > Overview“

Auf der Registerkarte **General > Overview** können Sie den Namen und die Beschreibung von Rollen bearbeiten, Sitzungs- und Benutzeroberflächen-optionen an- und ausschalten sowie Zugriffsfunktionen aktivieren. Wenn Sie eine Zugriffsfunktion aktivieren, müssen Sie auch entsprechende Ressourcenrichtlinien erstellen.

☑ **Verwalten allgemeiner Einstellungen und Optionen für Rollen**

So verwalten Sie allgemeine Einstellungen und Optionen für Rollen:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > General > Overview** aus.
2. Überprüfen Sie den Namen und die Beschreibung, und klicken Sie anschließend auf **Save Changes**. (Dies ist optional.)

3. Aktivieren Sie unter **Options** folgende Kontrollkästchen:
   - **Session Options**, um die auf der Registerkarte **General > Session Options** konfigurierten Einstellungen auf die Rolle anzuwenden.
   - **UI Options**, um die auf der Registerkarte **General > UI Options** konfigurierten Einstellungen auf die Rolle anzuwenden.
4. Aktivieren Sie unter **Access features** die für die Rolle vorgesehenen Funktionen. Folgende Optionen stehen zur Verfügung: Web, Dateien, Secure Application Manager (Windows- oder JAVAVERSION), Telnet/SSH, Konferenzen, E-Mail-Client und Network Connect.
5. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

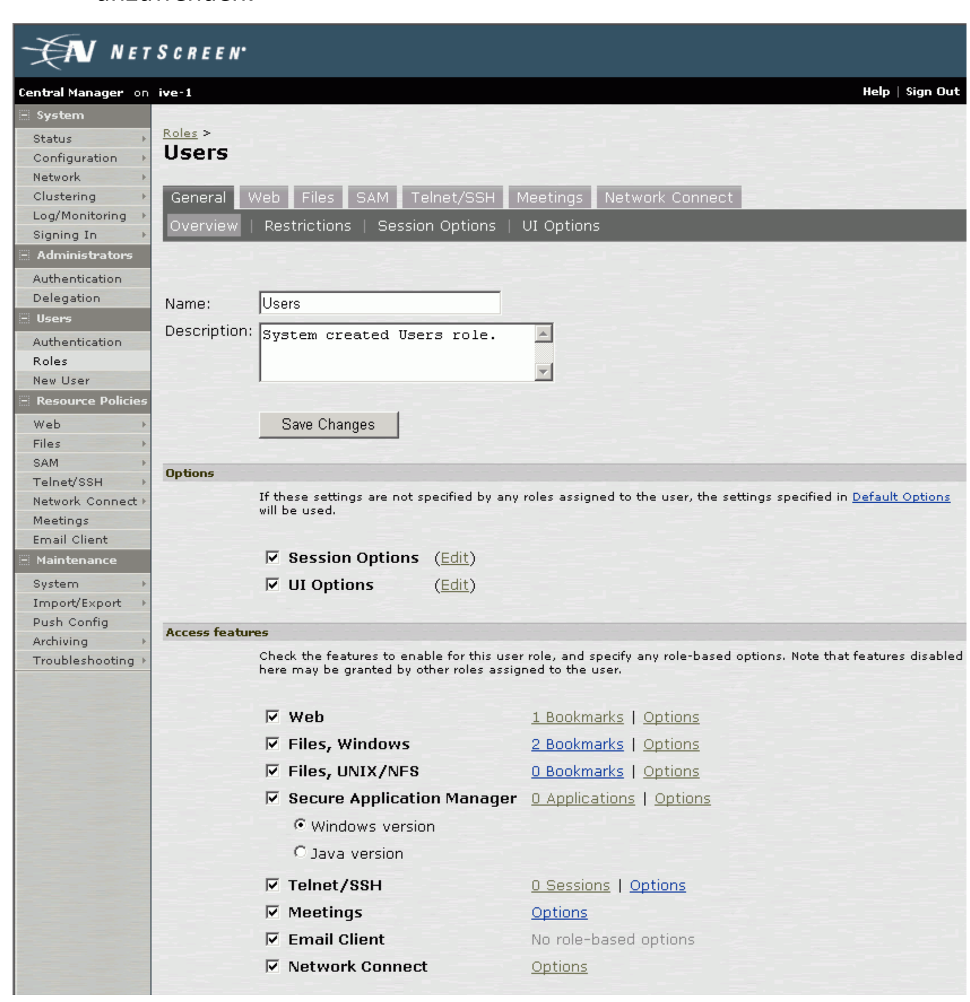


Abbildung 120: **Users > Roles > *Ausgewählte Rolle* > General > Overview**

Registerkarte „General > Restrictions“

Legen Sie auf der Registerkarte **General > Restrictions** Zugriffsverwaltungsoptionen für die Rolle fest. Das IVE berücksichtigt diese Beschränkungen, wenn es ermittelt, ob ein Benutzer einer Rolle zugeordnet wird. Benutzer werden der Rolle vom IVE nur dann zugeordnet, wenn Sie die angegebenen Beschränkungen erfüllen. Weitere Informationen zur Zugriffsverwaltung finden Sie unter : auf Seite 25.

☑ Festlegen von Zugriffsverwaltungsoptionen für die Rolle

So legen Sie Zugriffsverwaltungsoptionen für die Rolle fest:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > General > Restrictions** aus.
2. Klicken Sie auf die Registerkarte, die der Option entspricht, die Sie für die Rolle konfigurieren möchten:
   - Source IP Seite 584
   - Browser Seite 585
   - Certificate Seite 587
   - Host Checker Seite 590
   - Cache Cleaner Seite 591

   Für die Rolle kann eine beliebige Anzahl von Zugriffsverwaltungsoptionen konfiguriert werden. Wenn ein Benutzer nicht alle Beschränkungen erfüllt, ordnet das IVE ihn der Rolle nicht zu.

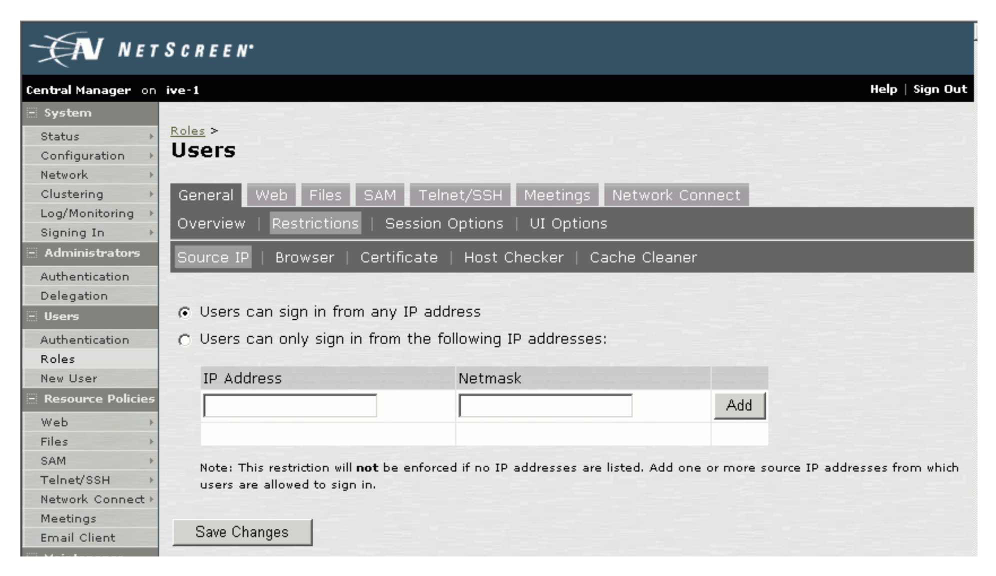


Abbildung 121: **Users > Roles > *Ausgewählte Rolle* > General > Restrictions**

Registerkarte „General > Session Options“

Auf der Registerkarte **General > Session** können Sie Sitzungszeitbegrenzungen, Roamingfunktionen, die Sitzungs- und Kennwortbeständigkeit, Optionen zur Anforderungsverfolgung sowie Anwendungsaktivitäten bei Leerlaufzeitüberschreitungen festlegen. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **Session Options**, um diese Einstellungen für die Rolle zu aktivieren.

☑ Angeben der Einstellungen für Benutzersitzungszeiten, Roaming, Beständigkeit und Anforderungen

So legen Sie allgemeine Sitzungsoptionen fest:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > General > Session Options** aus.
2. Geben Sie unter **Session Lifetime** Werte für folgende Optionen an:
   - **Idle Timeout** – Geben Sie die Anzahl der Minuten an, die sich eine nicht administrative Benutzersitzung im Leerlauf befinden kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Leerlaufzeitbegrenzung für Sitzungen beträgt in der Standardeinstellung zehn Minuten, d. h., eine Benutzersitzung, die zehn Minuten lang inaktiv ist, wird vom IVE beendet, und das Ereignis wird im Systemprotokoll protokolliert (sofern Sie nicht die unten beschriebenen Warnungen bei Sitzungszeitüberschreitung aktivieren).
   - **Max. Session Length** – Geben Sie die Anzahl der Minuten an, die eine aktive nicht administrative Benutzersitzung geöffnet bleiben kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Standardzeitbegrenzung für eine Benutzersitzung beträgt sechzig Minuten. Nach dieser Zeitspanne beendet das IVE die Benutzersitzung und protokolliert das Ereignis im Systemprotokoll.
   - **Reminder Time** – Geben Sie den Zeitpunkt an, zu dem das IVE Benutzer (außer Administratoren) wegen einer bevorstehenden Sitzungs- oder Leerlaufzeitüberschreitung warnen soll. Geben Sie die Anzahl von Minuten vor Erreichen der Überschreitung an.

3. Aktivieren Sie unter **Enable Session timeout warning** das Optionsfeld **Enabled**, um vor dem Erreichen der Sitzungszeitbegrenzung oder des Leerlaufzeitlimits auch andere Benutzer als Administratoren zu benachrichtigen. In diesen Warnungen werden Benutzer aufgefordert, kurz vor Erreichen der Sitzungsbegrenzung oder des Leerlaufzeitlimits eine geeignete Aktion durchzuführen, um gerade in Verarbeitung befindliche Formulardaten speichern zu können, die andernfalls verloren gehen würden. Benutzer, die sich dem Leerlaufzeitlimit nähern, werden zum Reaktivieren der Sitzung aufgefordert. Benutzer, die sich der Sitzungszeitbegrenzung nähern, werden zum Speichern der Daten aufgefordert.

   Ein IVE-Benutzer kann zum Beispiel bei der Arbeit mit einem für die Zusammenarbeit mit dem IVE konfigurierten E-Mail-Client unwissentlich das Leerlaufzeitlimit für seine Autorisierungsgruppe erreichen, da das IVE während des Verfassens der E-Mail keine Daten empfängt. Wenn Warnungen bei Sitzungszeitüberschreitung aktiviert sind, fordert das IVE den Benutzer jedoch auf, die IVE-Sitzung vor Ablauf der Zeitbegrenzung zu reaktivieren und erzwingt das Beenden der IVE-Sitzung des Benutzers. Diese Warnung gibt dem Benutzer die Möglichkeit, die teilweise verfasste E-Mail zu speichern.

4. Geben Sie unter **Roaming session** Folgendes an:

   - **Enabled** – Ermöglicht Roamingbenutzersitzungen für Benutzer, die dieser Gruppe zugeordnet sind. Eine Roamingbenutzersitzung funktioniert über Quell-IP-Adressen, wodurch sich mobile Benutzer (Benutzer von Laptops) mit dynamischen IP-Adressen von einem Standort aus im IVE anmelden können und Ihre Arbeit von einem anderen Standort fortsetzen können. Einige Browser weisen jedoch eventuell Schwachstellen auf, über die durch bösartigen Code Benutzercookies gestohlen werden können. Ein böswilliger Benutzer kann dann ein gestohlenes IVE-Sitzungscookie verwenden, um sich im IVE anzumelden.
   - **Limit to subnet** – Beschränkt die Roamingsitzung auf das lokale Subnetz, das im Feld **Netmask** angegeben ist. Benutzer können sich von einer IP-Adresse aus anmelden und ihre Sitzungen mit einer anderen IP-Adresse fortsetzen, sofern sich die neue IP-Adresse in demselben Subnetz befindet.
   - **Disabled** – Verbietet Roamingbenutzersitzungen für Benutzer, die dieser Rolle zugeordnet sind. Benutzer, die sich von einer IP-Adresse aus anmelden, können eine aktive IVE-Sitzung nicht von einer anderen IP-Adresse aus fortsetzen. Benutzersitzungen sind an die ursprüngliche Quell-IP-Adresse gebunden.

5. Aktivieren Sie unter **Persistent session** das Optionsfeld **Enabled**, um das IVE-Sitzungscookie auf die Festplatte des Clients zu schreiben, sodass die Anmeldeinformationen des IVE-Benutzers für die Dauer der IVE-Sitzung gespeichert werden.

   Standardmäßig wird das IVE-Sitzungscookie aus dem Speicher des Browsers gelöscht, wenn der Browser geschlossen wird. Die IVE-Sitzungsdauer wird sowohl vom Wert des Leerlaufzeitlimits als auch dem Wert der Höchstsitzungsdauer bestimmt, die Sie für die Rolle angeben. Die IVE-Sitzung wird nicht beendet, wenn ein Benutzer den Browser schließt. Eine IVE-Sitzung wird erst dann beendet, wenn sich ein Benutzer vom IVE abmeldet. Wenn ein Benutzer das Browserfenster schließt, ohne sich abzumelden, kann jeder beliebige Benutzer eine andere Instanz desselben Browsers öffnen, um auf das IVE zuzugreifen, ohne gültige Anmeldeinformationen zu senden.

   Hinweis: Wir empfehlen, diese Funktion nur für Rollen zu aktivieren, deren Mitglieder den Zugriff auf Anwendungen benötigen, für die IVE-Anmeldeinformationen erforderlich sind. Zudem sollten Sie dafür sorgen, dass sich diese Benutzer der Bedeutung der Abmeldung vom IVE nach Abschluss der Sitzung bewusst sind.

6. Aktivieren Sie unter **Persistent password caching** das Optionsfeld **Enabled**, damit zwischengespeicherte Kennwörter über mehrere Sitzungen für eine Gruppe erhalten bleiben können.

   Der IVE unterstützt die NTLM- und HTTP-Standardauthentifizierung sowie Server, die sowohl für NTLM-Anmeldungen als auch für anonyme Anmeldungen eingerichtet sind. Das IVE speichert von Benutzern eingegebene Kennwörter für die NTLM- und HTTP-Standardauthentifizierung im Cache, sodass die Benutzer nicht wiederholt aufgefordert werden, die Anmeldeinformationen einzugeben, die bereits bei der Anmeldung beim IVE-Server oder einer anderen Ressource in der NT-Domäne verwendet wurden. Standardmäßig leert der IVE-Server zwischengespeicherte Kennwörter aus dem Cache, wenn sich ein Benutzer abmeldet. Ein Benutzer kann zwischengespeicherte Kennwörter über die Seite **Advanced Preferences** löschen.
7. Aktivieren Sie unter **Browser request follow-through** das Optionsfeld **Enabled**, sodass Benutzeranforderungen vom IVE verarbeitet werden können, die nach Ablauf einer Benutzersitzung und erneuter Authentifizierung des Benutzers vorgenommen wurden.
8. Wählen Sie unter **Idle timeout application activity** die Option **Enabled** aus, damit durch Webanwendungen initiierte Aktivitäten (wie E-Mail-Abfragen) ignoriert werden, wenn ermittelt werden soll, ob eine Sitzung aktiv ist. Wenn Sie diese Option deaktivieren, kann durch regelmäßiges Ausführen von Ping-Befehlen oder durch andere Anwendungsaktivitäten das Überschreiten eines Leerlaufzeitlimits verhindert werden.
9. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

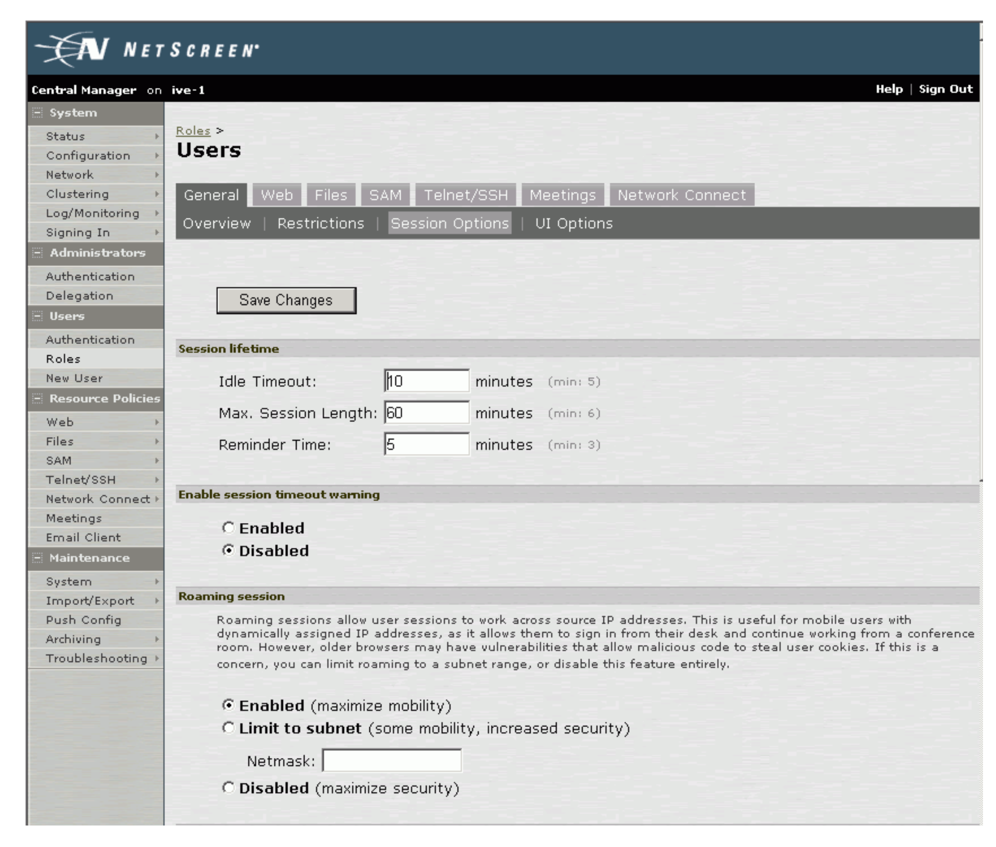


Abbildung 122: **Users > Roles > *Ausgewählte Rolle* > General > Session Options**

Registerkarte „General > UI Options“

Auf der Registerkarte **General > UI Options** können Sie benutzerdefinierte Einstellungen für die IVE-Willkommensseite angeben, die dieser Rolle zugeordneten Benutzern angezeigt wird. Die IVE-Willkommensseite (oder Startseite) ist die Weboberfläche, die authentifizierten IVE-Benutzern angezeigt wird. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **UI Options**, um diese Einstellungen für die Rolle zu aktivieren.

☑ Anpassen der IVE-Willkommensseite für Benutzer mit Rollen

So passen Sie die IVE-Willkommensseite für Benutzer mit Rollen an:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > General > UI Options** aus.
2. Ändern Sie in den Abschnitten **Custom Text** und **Custom Error Messages** den für die verschiedenen Fenstertitel verwendeten Standardtext nach Bedarf.
3. Legen Sie im Abschnitt **Header** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Seitenkopf fest.
4. Um Benutzern benutzerdefinierte Hilfeinformationen oder zusätzliche Anweisungen bereitzustellen, wählen Sie **Show Help Button**, geben Sie eine Beschriftung für die Schaltfläche ein, und legen Sie eine HTML-Datei fest, die in das IVE hochgeladen werden soll. Beachten Sie, dass im IVE keine Bilder und anderen Inhalte angezeigt werden, auf die auf dieser HTML-Seite verwiesen wird.
5. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden.
6. Klicken Sie auf **Restore Factory Defaults**, um die Darstellung der Anmeldeseite, der IVE-Startseite für Benutzer und der Webkonsole zurückzusetzen.

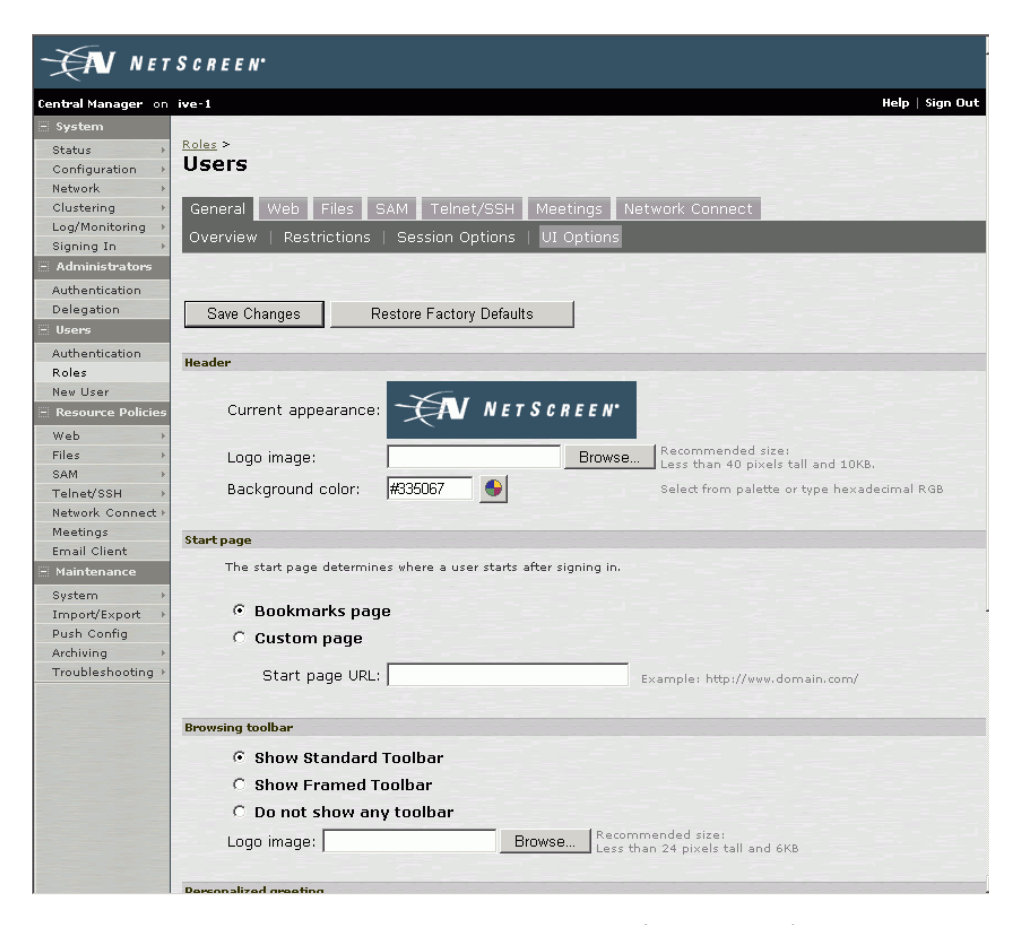


Abbildung 123: **Users > Roles >** ***Ausgewählte Rolle*** **> General > UI Options**

Registerkarte „Web > Bookmarks“

Auf der Registerkarte **Web > Bookmarks** können Sie Weblesezeichen erstellen, die dieser Rolle zugeordneten Benutzern auf der Willkommensseite angezeigt werden. Sie können den IVE-Benutzernamen eines Benutzers im URL-Pfad einfügen, um bei Einzelanmeldung den Zugriff auf Back-End-Webanwendungen zu ermöglichen.

☑ Erstellen von Lesezeichen für Webressourcen

So erstellen Sie ein Lesezeichen für eine Webressource:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Web > Bookmarks** aus.
2. Klicken Sie auf **New Bookmark**, und führen Sie auf der Seite **New Web Bookmark** Folgendes aus:
    1. Geben Sie einen Namen und eine Beschreibung für das Lesezeichen ein (optional). Diese Informationen werden anstelle des URLs auf der IVE-Startseite angezeigt.
    2. Geben Sie den URL für das Lesezeichen ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im URL `<USER>` (in Großbuchstaben) ein.
    3. Klicken Sie unter **Auto-allow** auf **Auto-allow Bookmark**, damit das IVE automatisch eine entsprechende Ressourcenrichtlinie für den Webzugriff erstellen kann. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:
        - **Only this URL**, um Benutzern nur den Zugriff auf den URL zu gestatten.
        - **Everything under this URL**, um Benutzern den Zugriff auf alle Pfade unter diesem URL zu gestatten.
3. Klicken Sie auf **Save** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

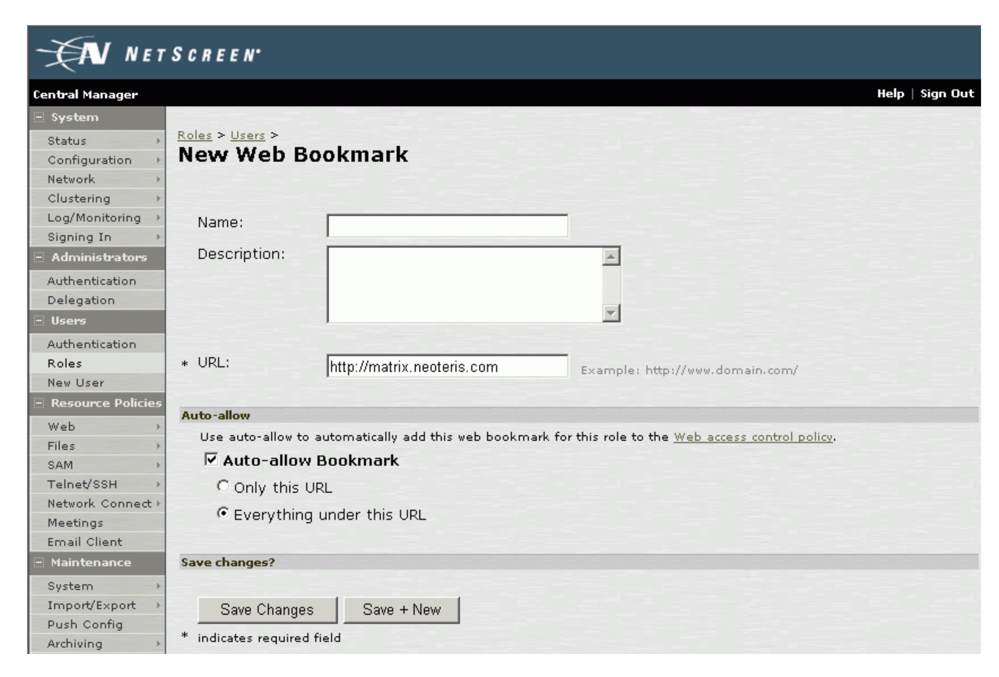


Abbildung 124: **Users > Roles > *Ausgewählte Rolle* > Web > Bookmarks > *New Bookmark***

Registerkarte „Web > Options“

Auf der Registerkarte **Web > Options** können Sie allgemeine Webbrowsingoptionen festlegen.

☑ Angeben von allgemeinen Webbrowsingoptionen

So geben Sie allgemeine Webbrowsingoptionen an:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Web > Options** aus.
2. Geben Sie unter **Browsing** die Optionen an, die für Benutzer aktiviert werden sollen:
   - **User can type URLs** – Diese Option ermöglicht es Benutzern, auf der Willkommensseite URLs einzugeben und zu Sites im Internet zu navigieren.
   - **Allow Java applets** – Diese Option ermöglicht es Benutzern, zu Webseiten zu navigieren, die clientseitige Java-Applets enthalten. Der IVE-Server wird für den Anwendungsserver wie ein Browser über SSL behandelt. Das IVE verarbeitet alle durch ein Java-Applet initiierten HTTP-Anforderungen und TCP-Verbindungen transparent und verarbeitet signierte Java-Applets.

     Wenn Sie diese Funktion aktivieren, können die Benutzer Java-Applets starten und Anwendungen ausführen, die als clientseitige Java-Applets implementiert wurden, z. B. VNC-Java-Client (Virtual Computing), Citrix NFuse Java-Client, WRQ Reflections Web-Client und Lotus WebMail. Diese Funktion wird zusammen mit den Ressourcenrichtlinien für die Java-Codesignatur verwendet.
   - **Mask hostnames while browsing** – Diese Option ermöglicht es Benutzern, Zielressouren im URL zu verbergen, die von Benutzern aufgerufen werden können. Wenn Sie die Option auswählen, werden die IP-Adressen und Hostnamen für den Benutzer an folgenden Stellen maskiert:
     - Adressleiste des Webbrowsers (wenn der Benutzer eine Seite aufruft)
     - Statusleiste des Webbrowsers (beim Führen des Mauszeigers über einen Hyperlink)
     - HTML-Quelldateien (wenn der Benutzer „View Source“ auswählt)

    - Durch die Hostnamen-Codierung wird verhindert, dass sich zufällige Besucher den URL einer internen Ressource notieren können. Dies erfolgt durch das Verbergen des Zielservers innerhalb des URLs, ohne dass dabei der vollständige Pfadname, die Zieldatei oder die Portnummer maskiert werden. Wenn ein Benutzer beispielsweise „www.msn.com" aufruft, ohne dass selektives Neuschreiben oder Hostnamencodierung aktiviert ist, wird der folgende URL in der Adressleiste des Webbrowsers des Benutzers angezeigt: http://www.msn.com/
  - **Unrewritten pages open in new window** – Wenn Benutzer auf Seiten zugreifen, die nicht neu geschrieben werden (siehe : auf Seite 457), erzwingt diese Option, dass der Inhalt in einem neuen Fenster angezeigt wird. So werden Benutzer daran erinnert, dass sie sich noch immer in einer sicheren Sitzung befinden.

3. Wählen Sie unter **Bookmarks** die Option **User can add bookmarks** aus, damit Benutzer auf der IVE-Willkommensseite persönliche Weblesezeichen erstellen können.
4. Aktivieren Sie unter **Cookies** die Option **Persistent cookies**, sodass Benutzer, die dieser Rolle angehören, ihre Browserumgebung durch Beibehaltung permanenter Cookies anpassen können. Standardmäßig löscht der IVE Webcookies, die während einer Benutzersitzung gespeichert wurden. Bei Aktivierung dieser Option können Benutzer Cookies über die Seite **Advanced Preferences** löschen.
5. Klicken Sie auf **Save Changes**.

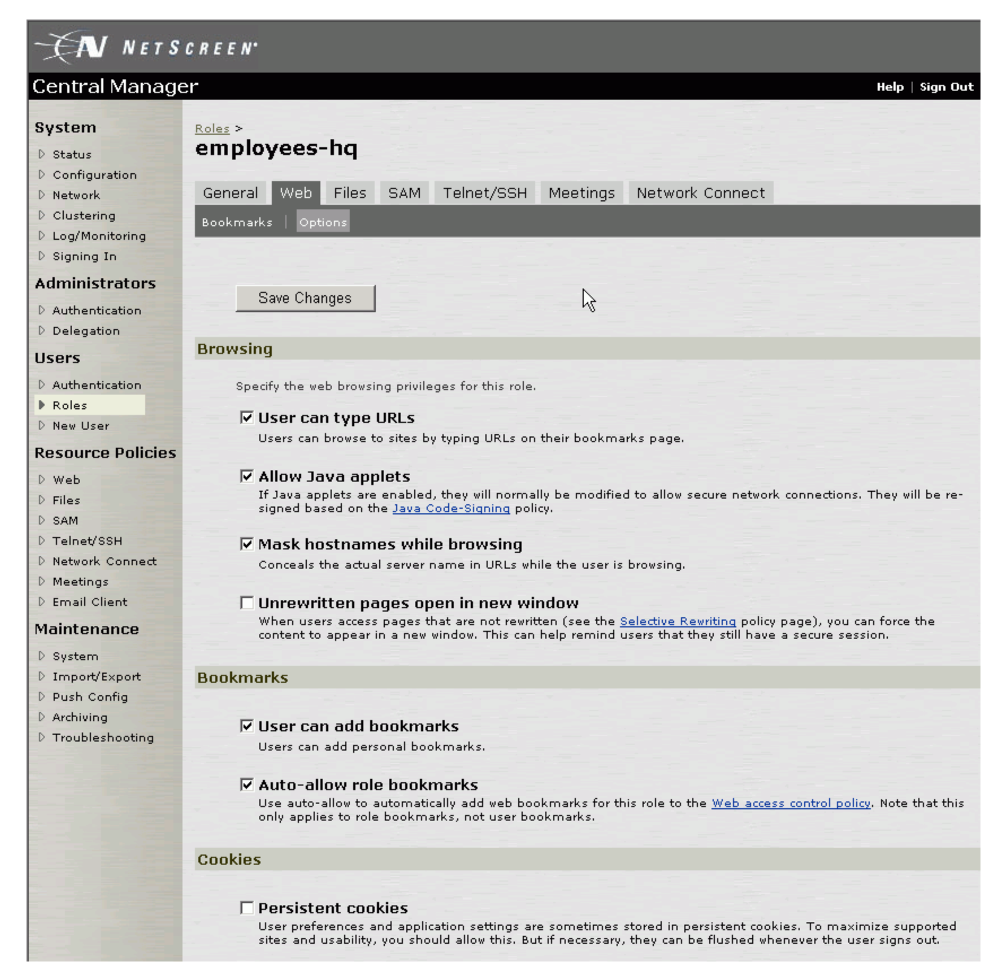


Abbildung 125: **Users > Roles > *Ausgewählte Rolle* > Web > Options**

Registerkarte „Files > Windows Bookmarks“

Auf der Registerkarte **Files > Windows Bookmarks** können Sie Windows-Lesezeichen erstellen, die dieser Rolle zugeordneten Benutzern auf der Willkommensseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

Wenn IVE-Benutzer zu Dateien auf einem Dfs-Server navigieren, gibt der Dfs-Server anhand der in Active Directory gespeicherten Site-Konfigurationsdaten Dfs-Verweise in der richtigen Reihenfolge an das IVE zurück. Verweise auf nähere Servers befinden sich in der Liste an einer höheren Position als Verweise auf weiter entfernte Server. Die Clients durchlaufen die Verweise in der Reihenfolge, in der diese empfangen werden. Wenn eine Anforderung von einem Client eingeht, der sich in einem nicht in der Liste aufgeführten Subnetz befindet, besitzt der Server keine Informationen über den Standort des Clients und gibt die Verweise in zufälliger Reihenfolge zurück. Auf diese Weise greifen Dfs-Anforderungen vom IVE (in diesem Falle in der Rolle des Clients) möglicherweise auf einen wesentlich weiter entfernten Server zu. Dies wiederum kann zu erheblichen Verzögerungen führen, insbesondere wenn das IVE versucht, auf einen Server zuzugreifen, der aus dem Subnetz mit dem IVE nicht erreichbar ist. Wenn das IVE in einem Subnetz installiert ist, das sich nicht in der Liste des Dfs-Servers befindet, kann der Dfs-Administrator das Subnetz mit dem IVE auf dem Domänencontroller mit dem Tool „Active Directory-Standorte und -Dienste“ zur entsprechenden Site hinzufügen.

☑ Erstellen von Lesezeichen für Windows-Ressourcen

So erstellen Sie ein Lesezeichen für eine Windows-Ressource:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Files > Windows Bookmarks** aus.
2. Klicken Sie auf **New Bookmark**, und wechseln Sie dann zum Server und Freigabenamen, bzw. geben Sie diesen ein. Geben Sie einen Pfad ein, um den Zugriff weiter einzuschränken. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad `<USER>` (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/der Freigabe auf der IVE-Startseite angezeigt.

Hinweis: Ein Windows-Server kann nicht mit einem Lesezeichen versehen werden. Sie müssen sowohl den Server- als auch den Freigabenamen angeben.

---

3. Wählen Sie für **Appearance** eine der folgenden Optionen aus:
   - **Appear as bookmark on homepage and in file browsing** – Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.
   - **Appear in file browsing only** – Das Lesezeichen wird dem Benutzer nur beim Navigieren durch Netzwerkdateien angezeigt.
4. Bei **Access** klicken Sie auf **Enable auto-allow access to this bookmark**, wenn das IVE automatisch eine entsprechende Ressourcenrichtlinie für Windows-Zugriff erstellen soll. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:
   - **Read-write access**, damit Benutzer Dateien auf dem Server speichern können.
   - **Include sub-folders**, damit Benutzer Dateien in den Verzeichnissen unter dem angegebenen Lesezeichenpfad anzeigen können.
5. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

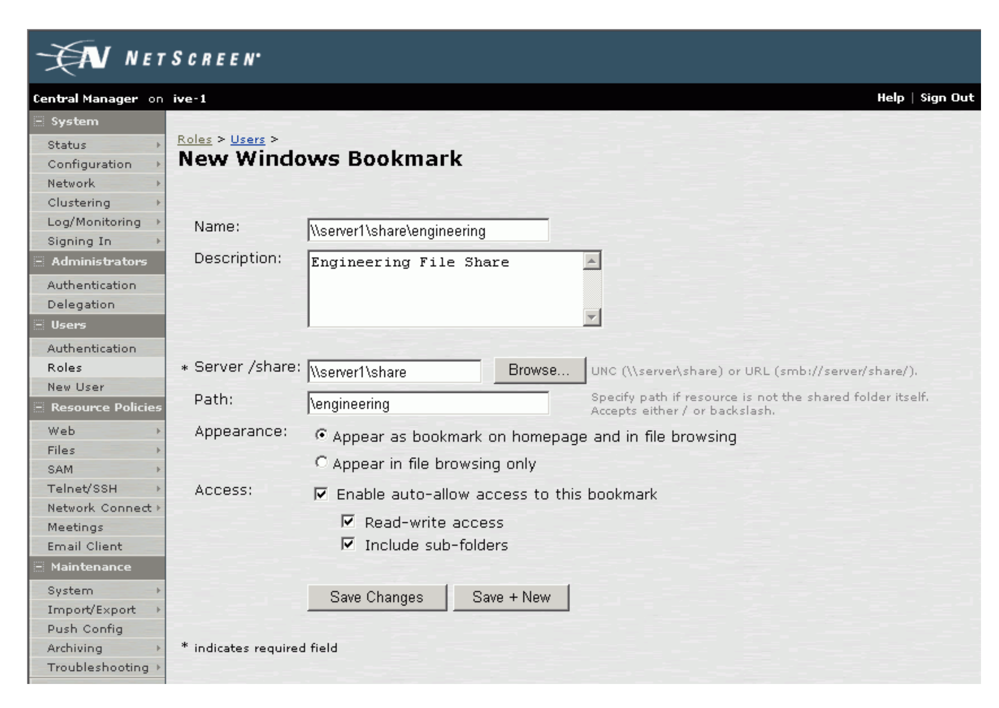


Abbildung 126: **Users > Roles > *Ausgewählte Rolle* > Files > Windows Bookmarks > *New Bookmark***

Registerkarte „Files > UNIX Bookmarks“

Auf der Registerkarte **Files > UNIX Bookmarks** können Sie UNIX/NFS-Lesezeichen erstellen, die auf der IVE-Startseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

☑ Erstellen von Lesezeichen für UNIX-Ressourcen

So erstellen Sie ein Lesezeichen für eine UNIX/NFS-Ressource:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Files > UNIX Bookmarks** aus.
2. Klicken Sie auf **New Bookmark**, und geben Sie den Hostnamen oder die IP-Adresse des Servers und den Pfad zu der Freigabe ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad <USER> (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/Pfades auf der IVE-Startseite angezeigt.
3. Wählen Sie für **Appearance** eine der folgenden Optionen aus:
   - **Appear as bookmark on homepage and in file browsing** – Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.
   - **Appear in file browsing only** – Das Lesezeichen wird dem Benutzer nur beim Navigieren durch Netzwerkdateien angezeigt.
4. Bei **Access** klicken Sie auf **Enable auto-allow access to this bookmark**, wenn das IVE automatisch eine entsprechende UNIX/NFS-Ressourcenrichtlinie erstellen soll. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt. Wählen Sie anschließend folgende Option aus:
   - **Read-write access**, damit Benutzer Dateien auf dem Server speichern können.
   - **Include sub-folders**, damit Benutzer Dateien in den Verzeichnissen unter dem angegebenen Lesezeichenpfad anzeigen können.
5. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

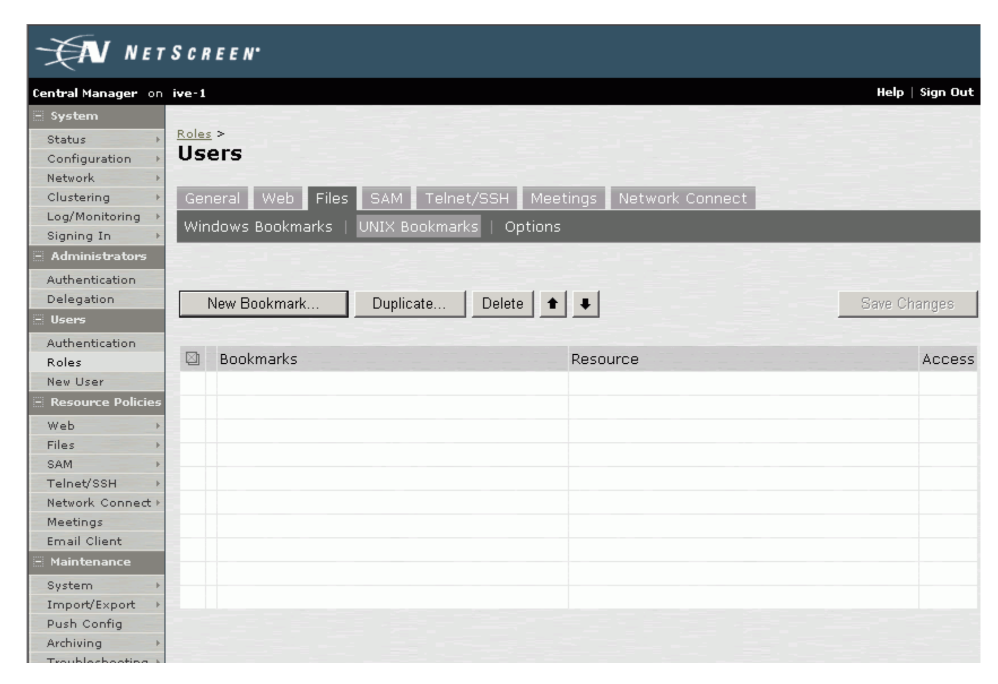


Abbildung 127: **Users > Roles > *Ausgewählte Rolle* > Files > UNIX Bookmarks**

Registerkarte „Files > Options"

Auf der Registerkarte **Files > Options** können Sie die Optionen zum Navigieren in Windows- und UNIX/NFS-Netzwerken angeben, einschließlich der Möglichkeit, Ressourcen anzuzeigen und Ordnerlesezeichen zu erstellen. Diese Optionen werden zusammen mit den Dateiressourcen-richtlinien verwendet.

☑ Angeben von allgemeinen Optionen zum Navigieren durch Dateien

So geben Sie allgemeine Optionen für die Dateinavigation an:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Web > Options** aus.

2. Geben Sie unter **Windows Network Files** die Optionen an, die für Benutzer aktiviert werden sollen:
   - **User can browse network file shares** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.
   - **User can add bookmarks** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.
3. Geben Sie unter **UNIX Network Files** die Optionen an, die für Benutzer aktiviert werden sollen:
   - **User can browse network file shares** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren UNIX-Dateifreigaben anzuzeigen und zu erstellen.
   - **User can add bookmarks** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.
   - **Allow automount shares** – Diese Option ermöglicht es Benutzern, auf Automount-Freigaben zuzugreifen, die auf einem NIS-Server angegeben sind.
4. Klicken Sie auf **Save Changes**.

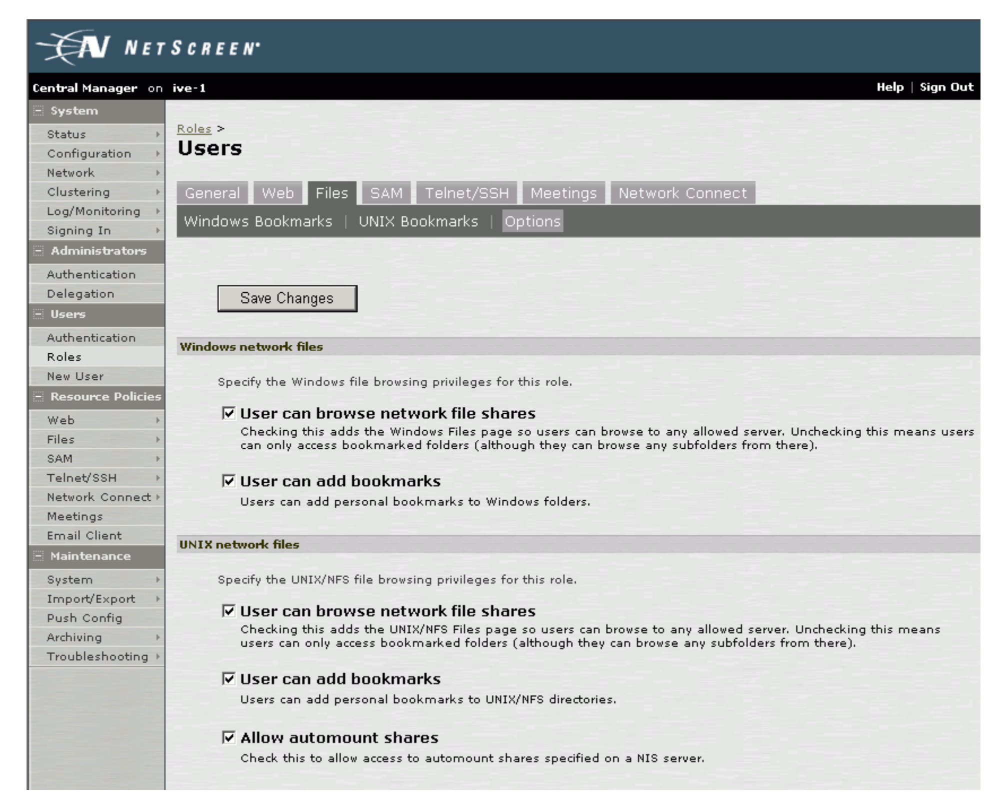


Abbildung 128: **Users > Roles > *Ausgewählte Rolle* > Files > Options**

Registerkarte „SAM > Applications“

Auf der Registerkarte **SAM > Applications** können Sie Client/Server-Anwendungen angeben, die von Secure Application Manager vermittelt werden sollen. Auf dieser Registerkarte werden je nach SAM-Version, die für die Rolle aktiviert ist, unterschiedliche Optionen angezeigt. Bei Aktivierung von:

- W-SAM, siehe : auf Seite 416
- J-SAM, siehe : auf Seite 416

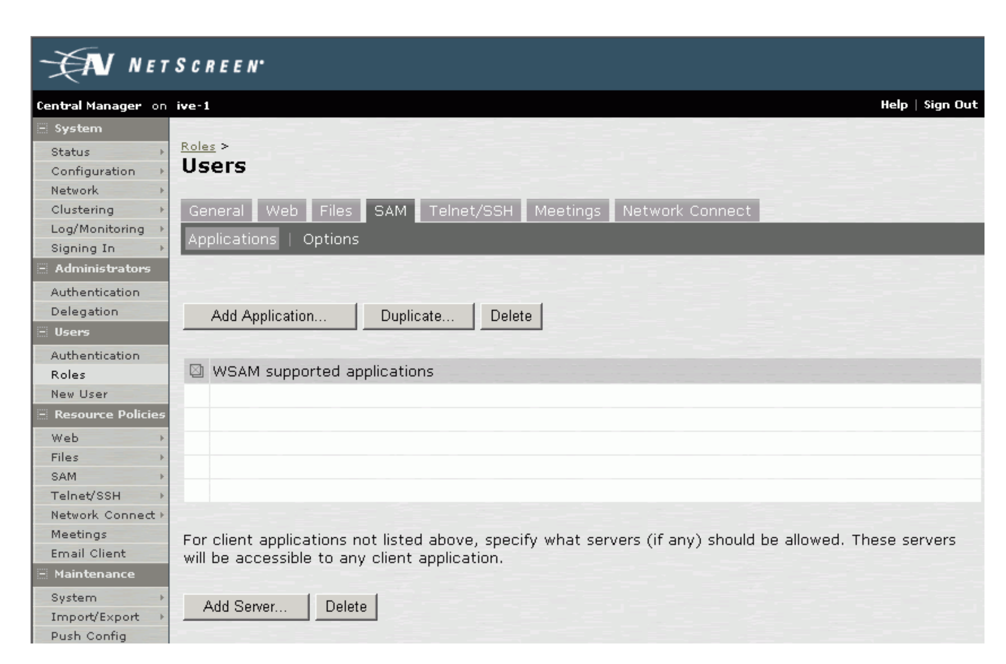


Abbildung 129: **Users > Roles > *Ausgewählte Rolle* > SAM > Applications**

☑ Angeben von Anwendungen und Servern, die mit W-SAM gesichert werden sollen

Auf der Registerkarte **Applications** können Sie Anwendungen und Server festlegen, für die W-SAM den Datenverkehr sichert. Wenn W-SAM auf einen Client-PC heruntergeladen wird, enthält dieser Informationen, die Sie für die Rolle auf der Registerkarte **Applications** konfiguriert haben. Nachdem ein Benutzer Secure Application Manager gestartet[1] hat, fängt W-SAM Anforderungen von Clientanwendungen an Server im internen Netzwerk und Anforderungen von auf dem Client ausgeführten Prozessen an interne Hosts ab. Sie legen diese Ressourcen auf der Registerkarte **Applications** fest, indem Sie zwei Listen konfigurieren:

- Liste **W-SAM supported applications**

  Diese Liste enthält Anwendungen, für die W-SAM den Client/Serververkehr zwischen dem Client und dem IVE sichern soll.

- Liste **W-SAM allowed servers**

  Diese Liste enthält Hosts, für die W-SAM den Client/Serververkehr zwischen dem Client und dem IVE sichern soll.

Wichtig: Wenn Sie anhand von W-SAM mit NetBIOS auf eine Freigabe zugreifen möchten, müssen Sie den NetBIOS-Namen des Servers (alphanumerische Zeichenfolge mit bis zu 15 Zeichen) an zwei Stellen explizit angeben: auf der Seite **Add Server** und in einer SAM-Ressourcenrichtlinie. (Gegenwärtig werden keine Platzhalter unterstützt.) Sie können auch auf der Registerkarte **SAM > Options** die Option **Auto-allow application servers** aktivieren, sodass das IVE automatisch eine SAM-Ressourcenrichtlinie erstellt, die den Zugriff auf diesen Server erlaubt.

So geben Sie Anwendungen und Server an, die mit W-SAM gesichert werden sollen:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles > *Ausgewählte Rolle* > SAM > Applications**.
2. Geben Sie Ressourcen aus der Liste **W-SAM supported application** an, für die W-SAM den Client/Server-Verkehr zwischen dem Client und dem IVE sichert:
   1 Klicken Sie auf **Add Application**.

---

1. Sie können Secure Application Manager so konfigurieren, dass er bei der Anmeldung eines Benutzers automatisch gestartet wird. Benutzer können diese Einstellung über das Menü IVE **System > Preferences** außer Kraft setzen. Wenn der automatische Start deaktiviert ist, muss Secure Application Manager manuell gestartet werden, indem auf die entsprechende Verknüpfung im IVE-Startseitenmenü geklickt wird.

2 Geben Sie den Namen der Anwendung und bei Bedarf eine Beschreibung ein. Diese Informationen werden auf der Seite „Client Applications“ für IVE-Benutzer angezeigt.

3 Wählen Sie eine der folgenden Optionen aus:

- **Standard application** – Auswahl von Citrix NFuse, Lotus Notes oder Microsoft Outlook/Exchange.
- **Custom application** – Angabe einer benutzerdefinierten Client/Server-Anwendung. Geben Sie im Feld **Filename** den Namen der ausführbaren Datei für die Datei an. Sie können darüber hinaus den Dateipfad und den MD5-Hash der ausführbaren Datei angeben. (Dies ist optional.)

  Wenn Sie einen MD5-Hash-Wert eingeben, überprüft W-SAM, ob der Prüfsummenwert der ausführbaren Datei diesem Wert entspricht. Wenn die Werte nicht übereinstimmen, teilt W-SAM dem Benutzer mit, dass die Identität der Anwendung nicht sichergestellt werden konnte, und leitet Verbindungen von der Anwendung zum IVE nicht weiter.

4 Klicken Sie auf **Save Changes** oder **Save + New**.

3. Geben Sie Ressourcen aus der Liste **W-SAM allowed servers** an, für die W-SAM den Client/Server-Verkehr zwischen dem Client und dem IVE sichert:

1 Klicken Sie auf **Add Servers**.

2 Geben Sie den Hostnamen (die Platzhalterzeichen „*“ oder „?“ sind zulässig) oder ein IP/Netzmaske-Paar an. Geben Sie mehrere Ports für einen Host als separate Einträge an.

3 Klicken Sie auf **Add**.

4. Legen Sie in einer Secure Application Manager-Ressourcenrichtlinie fest, an welche Unternehmensressourcen (basierend auf der Kombination aus IP-Adresse und Port) das IVE eine Anwendungs- oder Serveranforderung senden kann.

Sie können auch auf der Registerkarte **SAM > Options** die Option **Auto-allow application servers** aktivieren, sodass das IVE automatisch eine SAM-Ressourcenrichtlinie erstellt, die den Zugriff auf den angegebenen Server erlaubt. Beachten Sie, dass diese Option vor der Angabe der Anwendung bzw. des Servers aktiviert werden muss, andernfalls müssen Sie eine SAM-Ressourcenrichtlinie erstellen.

☑ Angeben von Anwendungen, die mit J-SAM gesichert werden sollen

Auf der Registerkarte **SAM > Applications** können Sie Anwendungen festlegen, für die J-SAM den Datenverkehr sichert. Beachten Sie, dass die Clientanwendung eine Verbindung mit dem lokalen Computer herstellen muss, auf dem Secure Application Manager als Anwendungsserver ausgeführt wird, damit die Java-Version von Secure Application Manager fehlerfrei verwendet werden kann. Die empfohlene Vorgehensweise für das Zuordnen von Anwendungsservern zum lokalen PC eines Benutzers besteht in der Aktivierung der automatischen Hostzuordnung, wodurch das IVE die Datei `hosts` automatisch so ändern kann, dass Anwendungsserver an den `lokalen Host` für sichere Portumleitung geleitet werden.

Wichtig: Die automatische Hostzuordnung kann auf Windows-PCs nur erfolgen, wenn die Benutzer über Administratorberechtigungen verfügen und Secure Application Manager daher die Datei `hosts` ändern kann. Wenn Benutzer nicht über Administratorrechte verfügen, wird im Secure Application Manager-Fenster eine Fehlermeldung angezeigt, und die Benutzer können nicht auf Client/Serveranwendungen zugreifen. Wenn die Sicherheitsrichtlinie das Erteilen von Administratorberechtigungen an Benutzer nicht zulässt, können Sie die externen DNS-Server auch wie unter : auf Seite 421 beschrieben konfigurieren.

Wenn J-SAM auf einen Clientcomputer heruntergeladen wird, enthält dieser Informationen, die Sie für die Rolle auf der Registerkarte **SAM > Applications** konfiguriert haben. Wenn ein Benutzer auf **Client Applications** klickt, wird J-SAM ausgeführt, fängt die Anforderungen an den festgelegten Ports ab und leitet sie über Ports an das IVE weiter. Das IVE leitet die Daten dann an den für den Anwendungsserver festgelegten Port weiter.

Hinweis

- Gegenwärtig wird auf Windows-, Linux- oder Macintosh-Plattformen Sun JVM, Version 1.4.1 oder höher unterstützt. Die MS JVM, die auf Sun JRE, Version 1.1 beruht, wird unter Windows ebenfalls unterstützt.
- Wenn Sie die Laufwerkzuordnung zu einem Server aktivieren möchten, müssen Sie Port 139 als Clientport und als Serverport für den betreffenden Server festlegen.

Für Windows XP-Benutzer wird von die Registrierung vom J-SAM automatisch geändert, um Port 445 zu deaktivieren, wodurch Windows XP zur Verwendung von Port 139 bei der Laufwerkzuordnung gezwungen wird. Benutzer von Windows XP müssen einen einmaligen Neustart ausführen, damit die Änderung an der Registrierung wirksam wird. Um die von J-SAM vorgenommene Registrierungsänderung zu deaktivieren, können Benutzer auf die Schaltfläche **Restore System Settings** auf der Seite IVE **Advanced Preferences** klicken. Wenn die Änderung wieder aktiviert werden soll, müssen sie einen Neustart ausführen.

So geben Sie Anwendungen an, die mit J-SAM gesichert werden sollen:

1. Wählen Sie in der Webkonsole die Optionen **Users > Roles > *Ausgewählte Rolle* > SAM > Applications**.
2. Geben Sie den Namen der Anwendung und bei Bedarf eine Beschreibung ein. Diese Informationen werden auf der Seite **Client Applications** für IVE-Benutzer angezeigt.
3. Wählen Sie eine der folgenden Optionen aus:
   - **Standard application** – Auswahl von Citrix NFuse, Lotus Notes oder Microsoft Outlook/Exchange.
   - **Custom application**
     1. Geben Sie im Feld **Server** den DNS-Namen oder die IP-Adresse des Servers ein.
     2. Geben Sie im Feld **Server Port** den Port ein, an dem der Remoteserver die Clientverbindungen überwacht.

        Wenn beispielsweise Telnet-Verkehr von einem Remotecomputer weitergeleitet werden soll, legen Sie sowohl für den Clientport (an dem J-SAM überwacht) als auch für den Serverport (an dem der Telnet-Server überwacht) Port 23 fest.

        Hinweis: Sie aktivieren die Laufwerkzuordnung zu dieser Ressource, indem Sie 139 als Serverport eingeben.
     3. Geben Sie im Feld **Local Port** den Port ein, den J-SAM auf Verbindungen mit Clientanwendungen überwachen soll.

        Normalerweise stimmt der Wert für den lokalen Port mit dem für den Serverport überein, er unterscheidet sich in der Regel nur für Linux- oder Macintosh-Benutzer, die Anwendungen für die Portweiterleitung hinzufügen möchten, die Ports unter 1024 verwenden.

        Hinweis: Sie aktivieren die Laufwerkzuordnung zu dieser Ressource, indem Sie 139 als Serverport eingeben.

Sie können mehrere Anwendungen an einem einzigen Port konfigurieren, beispielsweise `anw1.eigenefirma.com`, `anw2.eigenefirma.com`, `anw3.eigenefirma.com`. Das IVE weist jeder Anwendung eine Loopbackadresse (`127.0.1.10`, `127.0.1.11`, `127.0.1.12`) zu. J-SAM überwacht diese Loopbackadressen dann an dem festgelegten Port. Wenn beispielsweise Datenverkehr für die Adresse `127.0.1.12` am angegebenen Port vorhanden ist, leitet das IVE den Datenverkehr an den Zielhost `anw3.eigenefirma.com` weiter.

4 Aktivieren Sie das Kontrollkästchen **Allow Secure Application Manager to dynamically select an available port ...**, wenn J-SAM den gleichen Port auf mehrere Hosts überwacht und einen verfügbaren Port auswählen soll, falls der von Ihnen angegebene Clientport belegt ist. Um diese Option verwenden zu können, muss es die Clientanwendung ermöglichen, die Portnummer für die Verbindung festzulegen.

4. Klicken Sie auf **Save Changes** oder **Save + New**.

5. Wählen Sie unter **Enable Automatic Host Mapping (Java Version Only)** die Option **Enabled** aus, und klicken Sie dann auf **Save Changes**, wenn es sich bei den Benutzern um PC-Benutzer handelt.

   Clientanwendungen müssen Anwendungsserver zur IP-Adresse eines `localhost` auflösen. Wenn Sie die automatische Hostzuordnung für Benutzer von Remote-PCs nicht aktivieren möchten oder wenn es sich bei Ihren Benutzern um Linux-Benutzer handelt, müssen Sie Ihren externen DNS-Server zum Auflösen von Anwendungsservernamen zum `localhost` eines Benutzers konfigurieren. Detaillierte Informationen finden Sie unter : auf Seite 421.

6. Wenn der PC eines Remotebenutzers für die Verwendung eines Webproxys in Internet Explorer eingerichtet ist, konfigurieren Sie den Clientcomputer so, dass der Proxyserver umgangen wird, wenn der Benutzer Anwendungen startet, die eine Verbindung mit Secure Application Manager herstellen müssen. Weitere Informationen finden Sie unter : auf Seite 422.

7. Fügen Sie dem IVE DNS-Domänen hinzu, wenn Sie über mehrere interne Domänen verfügen (zum Beispiel `firma-a.com` und `firma-b.com`), sodass Namen wie zum Beispiel `anw1.firma-a.com` und `anw2.firma-b.com` ordnungsgemäß aufgelöst werden:

   1 Klicken Sie auf das Menü **Network > Network Settings**.

   2 Fügen Sie unter **DNS Name Resolution** im Feld **DNS Domains** eine durch Kommas getrennte Liste der Domänen hinzu.

   3 Klicken Sie auf **Save Changes**.

Zusätzliche Aufgaben für J-SAM

In diesem Abschnitt werden Aufgaben beschrieben, die Sie je nach den für J-SAM konfigurierten Client-/Serveranwendungen und dem von Ihren Benutzern verwendeten Betriebssystem möglicherweise durchführen müssen. Weiterhin enthält der Abschnitt Anweisungen zum Testen von J-SAM in Ihrem Unternehmen.

Folgende Themen werden behandelt:

☑ Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)

Clientanwendungen müssen Hostnamen von Servern zu J-SAM auflösen, wodurch Daten zwischen einem Client und einem Server über einen Proxy gesendet werden. Auf Windows-PCs werden Hostnamen von Servern in der Datei `hosts` gespeichert. Damit Daten mit J-SAM abgefangen werden können, müssen die Servernamen in dieser Datei zur Adresse des lokalen Computers (`localhost`) aufgelöst werden, sodass das IVE den Datenverkehr vermitteln kann. Bei der Zuordnung von Anwendungsservern zum lokalen PC eines Benutzers empfiehlt es sich, die automatische Hostzuordnung zu aktivieren (siehe Seite 425). Hierdurch erhält das IVE die Möglichkeit, die Datei `hosts` des PCs so zu ändern, dass Anwendungsserver auf den `localhost` des PCs verweisen, um eine sichere Portweiterleitung zu gewährleisten.

Das IVE kann nur automatische Hostzuweisung durchführen, wenn der PC-Benutzer auf dem Computer über Administratorrechte verfügt. Andernfalls müssen Sie sicherstellen, dass die internen Anwendungsservernamen extern zum `localhost` eines PCs aufgelöst werden. Fügen Sie hierfür entsprechende Einträge zu dem externen, mit dem Internet verbundenen DNS-Server hinzu (siehe folgende Beispiele):

```
127.0.0.1 anw1.firma-a.com
127.0.0.1 anw2.firma-b.de
127.0.0.1 exchange1.firma-a.de
127.0.0.1 exchange1.fima-b.de
```

Wenn die Clientanwendung einen unvollständigen Namen für den Anwendungsserver verwendet, müssen Benutzer DNS-Suffixe angeben, damit der PC das Suffix hinzufügen und für die Namensauflösung eine Verbindung mit dem externen DNS-Server herstellen kann. Ein Beispiel: Ein MS Outlook-Client hat üblicherweise einen unvollständigen Namen für einen MS Exchange-Server. Damit der unvollständige Name in die Adresse 127.0.0.1 aufgelöst werden kann, müssen Benutzer die entsprechenden DNS-Suffixe auf ihren PCs angeben. Das Hinzufügen von Domänennamen wirkt sich nicht auf andere Vorgänge auf dem PC aus, einschließlich der Verwendung der Clientanwendung innerhalb des Unternehmens.

So konfigurieren Sie einen Benutzer-PC mit DNS-Suffixen (Windows 2000):

1. Wählen Sie im **Startmenü** von Windows **Einstellungen > Netzwerk- und DFÜ-Verbindungen > LAN-Verbindung** und dann **Eigenschaften** aus.
2. Wählen Sie **Internetprotokoll (TCP/IP)** aus, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
4. Klicken Sie auf **Diese DNS-Suffixe anhängen** und dann auf **Hinzufügen**.
5. Fügen Sie die internen Domänen Ihres Unternehmens als zusätzliche DNS-Suffixe hinzu.

☑ Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt

Dieses Verfahren kann jedoch nur angewendet werden, wenn der PC eines Remotebenutzers so konfiguriert ist, dass in Internet Explorer ein Webproxy verwendet wird. Dieses Verfahren gewährleistet, dass Clientanwendungen eine Verbindung mit Secure Application Manager herstellen, statt zu versuchen, eine Verbindung mit dem Webproxy herzustellen.

So konfigurieren Sie einen PC, der in Internet Explorer eine Verbindung mit dem IVE über einen Webproxy herstellt:

1. Wählen Sie in Internet Explorer im Menü **Extras** die Option **Internetoptionen** aus.
2. Klicken Sie auf der Registerkarte **Verbindungen** auf die Schaltfläche **LAN-Einstellungen**.
3. Klicken Sie unter **Proxyserver** auf die Schaltfläche **Erweitert**.

4. Geben Sie unter Ausnahmen die Adressen ein, für die kein Proxyserver verwendet werden soll. Geben Sie alle Adressen (Hostnamen und `localhost`) ein, die die Clientanwendung beim Herstellen einer Verbindung über Secure Application Manager verwendet.

   Beispiele:

   Wenn der Anwendungsserver den Namen `anw1.firma.com` hat, geben Sie die folgenden Ausnahmen ein:

   ```
   anw1;anw1.firma.de;127.0.0.1
   ```

   Wenn der Exchange-Server den Namen `exchange.firma.com` hat, geben Sie die folgenden Ausnahmen ein:

   ```
   exchange;exchange.firma.de;127.0.0.1
   ```

Registerkarte „SAM > Options“

Verwenden Sie die Registerkarte **SAM > Options** , um Folgendes durchzuführen:

☑ Angeben allgemeiner Optionen für Secure Application Manager

So legen Sie allgemeine Secure Application Manager-Optionen fest:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > SAM > Options** aus.
2. Legen Sie unter **Secure Application Manager options** die Optionen fest, die für Benutzer aktiviert werden sollen:
   - **Auto-launch Secure Application Manager** – Wenn diese Option aktiviert ist, startet das IVE Secure Application Manager automatisch, wenn sich ein Benutzer anmeldet. Wenn die Option nicht aktiviert wird, müssen Benutzer Secure Application Manager im Menü **Client Applications** manuell starten.
   - **Auto-uninstall Secure Application Manager** – Wenn diese Option aktiviert ist, deinstalliert das IVE Secure Application Manager automatisch nach der Abmeldung des Benutzers.
   - **Auto-allow application servers** – Wenn diese Option aktiviert ist, erstellt das IVE automatisch eine SAM-Ressourcenrichtlinie, die den Zugriff auf den in der Liste für W-SAM-Anwendungen und -Server sowie in der Liste der J-SAM-Anwendungen angegebenen Server zulässt.
3. Klicken Sie auf **Save Changes**.

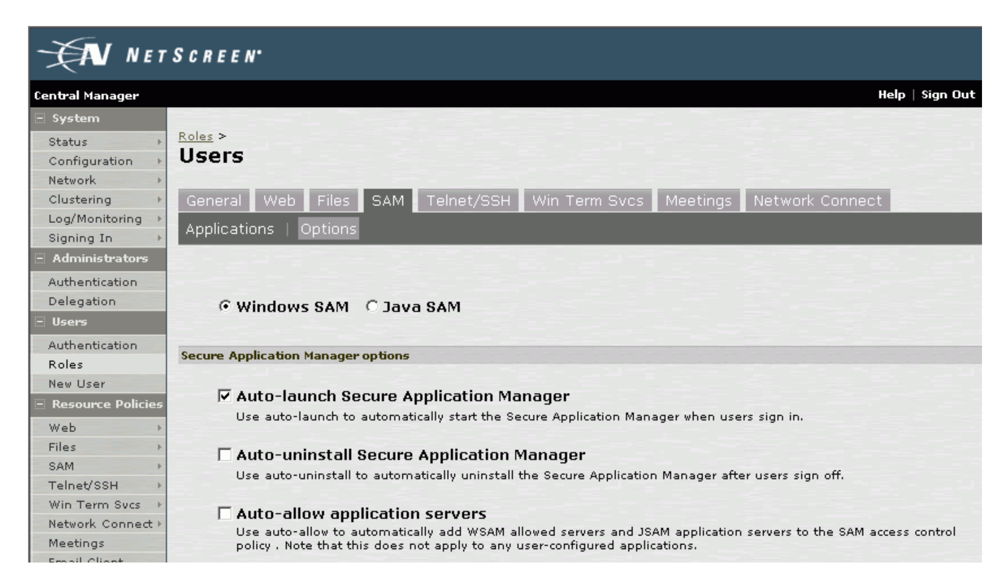


Abbildung 130: **Users > Roles > *Ausgewählte Rolle* > SAM > Options – General Options**

☑ Angeben von Windows Secure Application Manager-Optionen

So geben Sie Windows Secure Application Manager-Optionen an:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > SAM > Options** aus.
2. Führen Sie unter **Windows SAM Options** Folgendes aus:
   1 Wählen Sie **Auto-upgrade Secure Application Manager** aus, wenn das IVE Secure Application Manager automatisch auf einen Clientcomputer herunterladen soll, sofern die Secure Application Manager-Version auf dem IVE neuer als die auf dem Clientcomputer installierte Version ist. Beachten Sie bei Auswahl dieser Option Folgendes:
      - Benutzer müssen über Administratorberechtigungen verfügen, damit das IVE Secure Application Manager automatisch auf dem Client installiert.
      - Wenn ein Benutzer Secure Application Manager deinstalliert und sich anschließend bei einem IVE anmeldet, für das die Option **Auto-upgrade Secure Application Manager** nicht aktiviert ist, kann er nicht mehr auf Secure Application Manager zugreifen.

2 Geben Sie den Pfad und den Dateinamen einer Batch-, Anwendungs- oder Win32-Dienstdatei ein, die nach Beginn bzw. Ende einer W-SAM-Sitzung ausgeführt werden soll. Wenn Sie beispielsweise eine Anwendung beenden und anschließend neu starten möchten, können Sie „PSKILL.exe" verwenden. Diese Datei muss auf dem Client installiert bzw. in einem zugänglichen Netzwerkverzeichnis gespeichert sein und das W-SAM-Startprogramm aufrufen.

Hinweis: Sie können Windows-Variablen verwenden (wie in „path%WINDIR%\system32\log"), um sicherzustellen, dass die Datei auf verschiedenen Plattformen vom IVE gefunden werden kann.

---

3. Klicken Sie auf **Save Changes**.

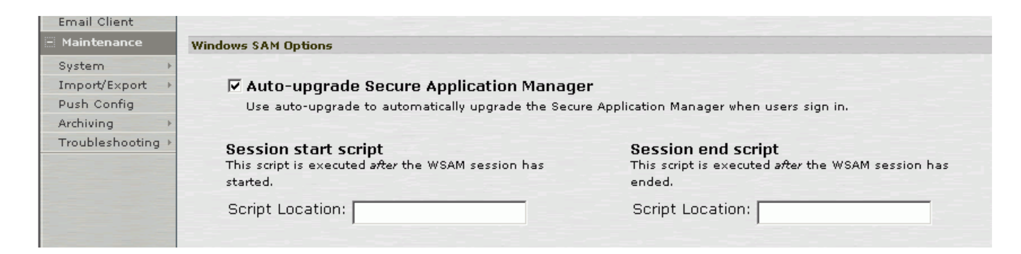


Abbildung 131: **Users > Roles > *Ausgewählte Rolle* > SAM > Options - W-SAM Options**

☑ Herunterladen von Windows Secure Application Manager-Anwendungen

Sie können Windows Secure Application Manager als ausführbare Datei herunterladen, die Ihnen folgende Möglichkeiten bietet:

- Verteilen der Datei auf mehrere Clientcomputer mithilfe von Softwareverteilungstools. Mit dieser Option können Sie W-SAM auf Clientcomputern installieren, deren Benutzer nicht über die zum Installieren von W-SAMerforderlichen Administratorrechte verfügen.
- Bereitstellen der ausführbaren Datei in einem sicheren Repository, damit Benutzer die richtige Version herunterladen und installieren können.

Mit diesen Optionen können Sie steuern, welche Version von W-SAM auf Clientcomputern ausgeführt wird. Beachten Sie, dass das IVE drei herunterladbare Versionen von W-SAM bereitstellt:

- **Eigenständiges WSAM-Installationsprogramm** – Dieses Installationsprogramm enthält die Standardversion von W-SAM.
- **Eigenständiges Installationsprogramm für WSAM mit NetBios** – Dieses Installationsprogramm enthält die NetBIOS-Version von W-SAM, die es Benutzern ermöglicht, Laufwerke zu Windows-Ressourcen zuzuordnen.
- **Skriptfähiges WSAM-Startprogramm** – Mithilfe diese Tools kann W-SAM entweder manuell über die Befehlszeile eines PCs oder durch automatischen Aufruf gestartet werden, z. B. über eine Batchdatei, eine einen Shellaufruf ausführende Anwendung oder einen Win32-Dienst. Informationen zu Befehlszeilenargumenten, Rückgabecodes, Fehler und Beispielen finden Sie in Anhang F.: auf Seite 641.

Wichtig: Wenn Sie W-SAM verteilen möchten, ist zu empfehlen, die Option **Auto-upgrade Secure Application Manager** zu deaktivieren. Wenn diese Option aktiviert ist, wird vom IVE automatisch eine neuere Version von W-SAM auf den Client heruntergeladen, was dazu führt, dass verschiedene Benutzer uneinheitliche Versionen von W-SAM ausführen. Wenn Benutzer nicht über Administratorberechtigungen verfügen, schlägt die Aktualisierung außerdem fehl, und WSAM kann ggf. nicht mehr ordnungsgemäß ausgeführt werden.

So laden Sie ein W-SAM-Installationsprogramm herunter:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > SAM > Options** aus.
2. Klicken Sie unter **Downloads** auf die Verknüpfung für das gewünschte Installationsprogramm, um die ausführbare W-SAM-Datei vom IVE herunterzuladen.
3. Deaktivieren Sie unter **Windows SAM Options** die Option **Auto-upgrade Secure Application Manager**, um sicherzustellen, dass W-SAM vom IVE nicht auf Clientcomputer heruntergeladen wird (optional).
4. Klicken Sie auf **Save Changes**.

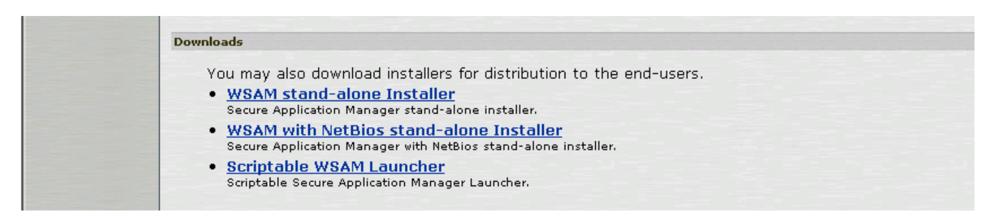


Abbildung 132: **Users > Roles > *Ausgewählte Rolle* > SAM > Options - SAM-Downloads**

☑ Angeben von Java Secure Application Manager-Optionen

So geben Sie Java Secure Application Manager-Optionen an:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > SAM > Options** aus.
2. Legen Sie unter **Java SAM Options** die Optionen fest, die für Benutzer aktiviert werden sollen:
   - **User can add applications** – Diese Option ermöglicht Benutzern das Hinzufügen von Anwendungen. Damit Benutzer Anwendungen hinzufügen können, müssen Sie den DNS-Namen und die Client/Serverports des Anwendungsservers kennen.

     Wenn Sie diese Option aktivieren, können Benutzer die Portumleitung zu einem beliebigen Host oder Port im Unternehmen einrichten. Bevor Sie Benutzern die Möglichkeit geben, Anwendungen hinzuzufügen, vergewissern Sie sich, dass diese Funktion mit Ihren Sicherheitsanforderungen vereinbar ist. Wenn ein Benutzer eine Anwendung hinzufügt, bleibt diese für den Benutzer auch dann verfügbar, wenn die Funktion später deaktiviert wird.

- **Automatic host-mapping** – Diese Option ermöglicht es Secure Application Manager, die Datei „hosts" des Windows-PCs zu bearbeiten und Einträge von Windows-Anwendungsservern durch localhost zu ersetzen. Diese Einträge werden auf die Originaldaten zurückgesetzt, wenn ein Benutzer Secure Application Manager schließt.

  Die Java-Version von Secure Application Manager kann nur dann verwendet werden, wenn zwischen der Clientanwendung und dem lokalen PC, auf dem Secure Application Manager als Anwendungsserver ausgeführt wird, eine Verbindung eingerichtet wird. Bei der Zuordnung von Anwendungsservern zum lokalen PC eines Benutzers empfiehlt es sich, die automatische Hostzuordnung zu aktivieren. Das IVE kann dann die Datei „hosts" automatisch so ändern, dass Anwendungsserver für sichere Portumleitung zum lokalen Host des PCs geleitet werden. Sie können auch den externen DNS-Server konfigurieren.
- **Skip web-proxy registry check** – Wenn diese Option aktiviert ist, überprüft J-SAM die Registrierung des Benutzers nicht auf einen Webproxy. Manche Benutzer sind nicht berechtigt, die eigene Registrierung einzusehen. Wenn J-SAM versucht, die Registrierung aufzurufen, kann dem Benutzer daher ein Fehler aufgrund fehlender Berechtigungen angezeigt werden. Die Auswahl dieser Option gewährleistet, dass Benutzern diese Meldung nicht angezeigt wird.
- **Auto-close JSAM window on sign-out** – Wenn diese Option aktiviert ist, wird J-SAM automatisch geschlossen, sobald sich ein Benutzer vom IVE abmeldet, indem er im IVE-Browserfenster auf **Sign Out** klickt. Wenn nur das Browserfenster geschlossen wird, wird J-SAM weiterhin ausgeführt.

3. Klicken Sie auf **Save Changes**.

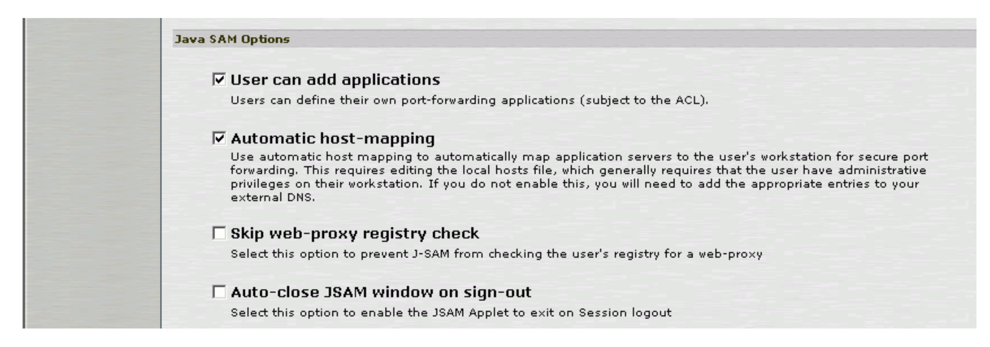


Abbildung 133: **Users > Roles > *Ausgewählte Rolle* > SAM > Options — J-SAM Options**

Registerkarte „Telnet/SSH > Sessions“

Auf der Registerkarte **Telnet/SSH > Sessions** können Sie Lesezeichen für sichere Terminalsitzungen erstellen, die dieser Rolle zugeordneten Benutzern auf der Willkommensseite angezeigt werden. In Lesezeichen für Terminalsitzungen sind Informationen zu Terminalsitzungen für Telnet- oder SSH-Sitzungen festgelegt, die von Benutzer gestartet werden können Diese Sitzungen gewähren Benutzern Zugriff auf eine Reihe von vernetzten Geräten, beispielsweise UNIX-Server, Netzwerkgeräte und andere Legacyanwendungen, die Terminalsitzungen verwenden.

Wenn Sie die Aktualisierungsoption Secure Terminal Access aktivieren (Telnet/SSH), den Benutzern jedoch nicht die Möglichkeit bieten, eigene Lesezeichen zu erstellen Seite 431, müssen Sie unbedingt die Sitzungslesezeichen für sie konfigurieren. Andernfalls können Benutzer diese Funktion nicht nutzen.

Die Benutzer können den mit benutzerdefinierten Parametern erstellten URL kopieren und in jedes Webdokument einfügen, wenn sie anderen Benutzern den Zugriff auf eine Telnet- oder SSH-Sitzung gewähren möchten.

Hinweis: Gegenwärtig wird die Sun JVM in der Version 1.4.1 oder höher unterstützt.

☑ Erstellen von Lesezeichen für sichere Terminalsitzungen

So erstellen Sie Lesezeichen für sichere Terminalsitzungen:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Telnet/SSH > Sessions** aus.
2. Klicken Sie auf **Add Session**, und geben Sie die erforderlichen Informationen ein, die durch ein Sternchen (*) gekennzeichnet sind. Wenn Sie einen Namen und eine Beschreibung für ein Lesezeichen angeben, werden diese Informationen auf der Seite **Terminal Sessions** angezeigt.
3. Klicken Sie auf **Save Changes** oder **Save + New**.

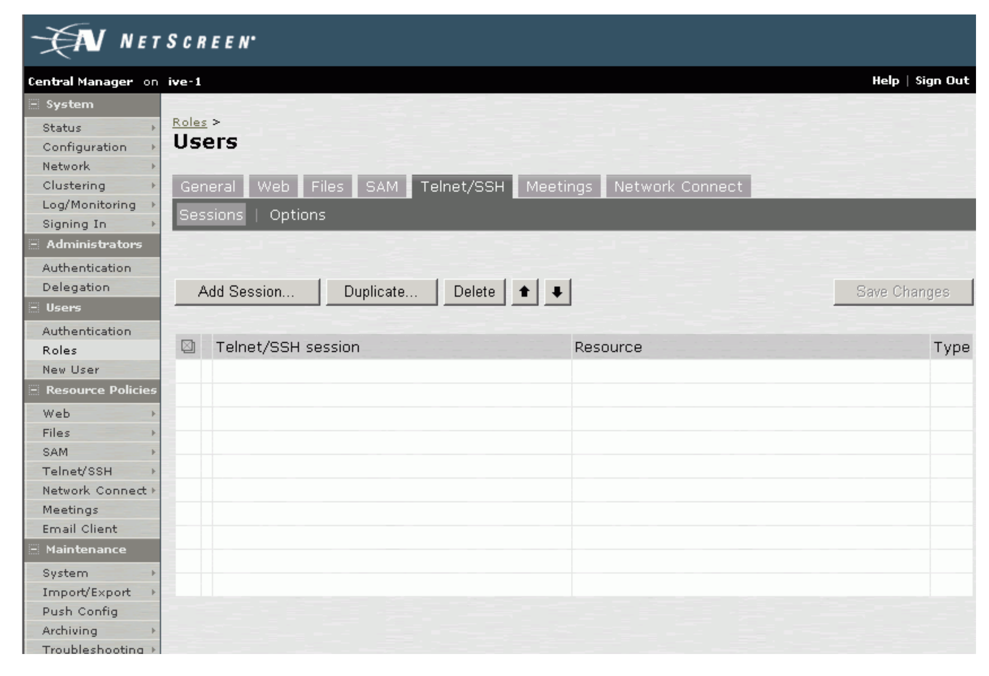


Abbildung 134: **Users > Roles > *Ausgewählte Rolle* > Telnet/SSH > Sessions**

Registerkarte „Telnet/SSH > Options“

Auf der Registerkarte **Telnet/SSH > Options** können Sie es den Benutzern ermöglichen, eigene Telnet/SSH-Lesezeichen zu erstellen, zu einer Terminalsitzung zu navigieren und das IVE so zu konfigurieren, dass Telnet/SSH-Ressourcenrichtlinien erstellt werden, die den Zugriff auf die in den Sitzungslesezeichen angegebenen Server gewähren.

Wenn Sie Benutzern das Navigieren zu einer Terminalsitzung ermöglichen, ist zu beachten, dass dies auf zweierlei Weise erfolgen kann:

- **Über die IVE-Startseite**

  Die Benutzer können den Server und den Port für den Zugriff auf der IVE-Startseite im Feld **Address** eingeben. Dabei sind folgende URL-Formate gültig:

  - Telnet://host:port
  - SSH://host:port

  Beispiel: `Telnet://terminalserver.eigenefirma.com:3389`

- **Über die Adressleiste des Webbrowsers**

  Die Benutzer können den Server und den Port für den Zugriff (sowie Sitzungsparameter wie Schriftart und Fenstergröße) in der Adressleiste des Webbrowsers mithilfe des Standardwebprotokolls eingeben. Beispiel:

  ```
  https://iveserver/dana/term/newlaunchterm.cgi?protocol=telnet&host=
  termsrv.yourcompany.com&port=23&username=jdoe&fontsize=12&buffer=80
  0&size=80x25
  ```

☑ Angeben allgemeiner Optionen für Telnet/SSH

So geben Sie allgemeine Optionen für Telnet/SSH an:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Telnet/SSH > Options** aus.
2. Aktivieren Sie die Option **User can add sessions**, damit Benutzer eigene Sitzungslesezeichen definieren können und anhand der Syntax `telnet://` und `ssh://` sowie `/dana/term/newlaunchterm.cgi` zu einer Terminalsitzung navigieren können. Wenn Sie diese Option aktivieren, wird auf der Seite **Terminal Sessions** die Schaltfläche **Add Terminal Session** angezeigt, wenn ein Benutzer die IVE-Willkommensseite das nächste Mal aktualisiert.
3. Aktivieren Sie die Option **Auto-allow role Telnet/SSH sessions**, damit durch das IVE automatische der Zugriff auf die im Sitzungslesezeichen definierten Ressourcen gewährt wird (und keine Ressourcenrichtlinien erstellt werden müssen). Beachten Sie, dass dies nur für Rollenlese-zeichen und nicht für Benutzerlesezeichen gilt.
4. Klicken Sie auf **Save Changes**.

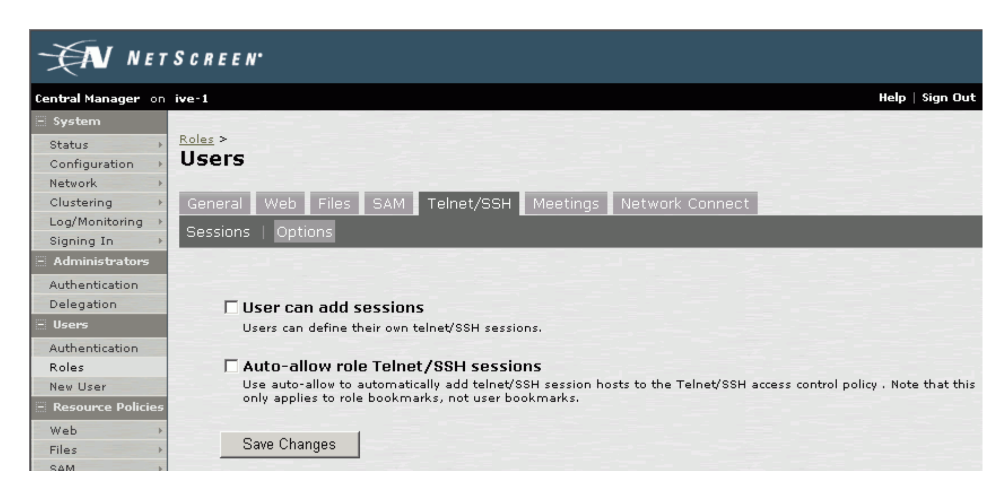


Abbildung 135: **Users > Roles > *Ausgewählte Rolle* > Telnet/SSH > Options**

Registerkarte „Meetings“

Auf der Registerkarte **Meetings** können Sie zu einem beliebigen Zeitpunkt festlegen, welche Benutzerrollen Konferenzen planen können (siehe unter : auf Seite 15), um die Sicherheitsstufen für die zu erstellenden Konferenzen zu steuern und um die für Konferenzen verwendeten Systemressourcen zu verwalten.

Beachten Sie bei der Erstellung von Benutzerrollen Folgendes: Wenn Benutzer mehreren Rollen zugeordnet sind und Sie diese zusammenführen Seite 58, werden alle Optionen auf der Seite **User > Roles > Meetings** mit Ausnahme der Richtlinieneinstellungen zusammengeführt, sodass Sie erweiterten Zugriff gewähren, der jedoch zu Lasten der Sicherheit geht. Wenn die Richtlinieneinstellungen angewendet werden, die die Anzahl der Konferenzen und der pro Rolle zulässigen Teilnehmer steuern, durchläuft Secure Meeting die verschiedenen Rollen, um solche zu finden, deren Höchstzahl noch nicht erreicht ist.

Sie können z. B. festlegen, dass die folgenden Rollen die angegebene Anzahl von Konferenzen planen können:

- Entwicklung: 25 Konferenzen
- Management: 50 Konferenzen
- Vertrieb: 200 Konferenzen

Wenn Joe diesen Rollen (in der genannten Reihenfolge) zugeordnet ist und versucht, eine Konferenz zu planen, überprüft Secure Meeting zunächst, ob die zulässige Anzahl geplanter Konferenzen für die Rolle „Entwicklung“ bereits erreicht ist. Wenn dies der Fall ist, überprüft Secure Meeting die Konferenzanzahl für die Rolle „Management“. Wenn auch hier die Höchstzahl erreicht ist, überprüft Secure Meeting diejenige für die Rolle „Vertrieb“. Nur wenn die Höchstzahl für alle Rollen erreicht ist, wird Joe von Secure Meeting eine Meldung angezeigt, dass die Höchstzahl geplanter Konferenzen erreicht ist und er keine Konferenz erstellen kann. Die Anzahl von Konferenzen oder Konferenzteilnehmern kann nicht auf Bereichsebene begrenzt werden.

☑ Aktivieren und Konfigurieren von Konferenzen für Benutzerrollen

So aktivieren und konfigurieren Sie Konferenzen:

1. Wählen Sie in der Webkonsole **Users > Roles** aus.
2. Wählen Sie eine Rolle aus.

3. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **Meetings**, und klicken Sie auf **Save Changes**.

Wichtig: Wenn Sie das Kontrollkästchen **Meetings** nicht aktivieren, können Benutzer keine Konferenzen erstellen oder planen und die Seite **Meetings** nicht anzeigen. Sie können jedoch trotzdem an den Konferenzen teilnehmen, zu denen sie eingeladen sind. Dazu klicken sie auf die Verknüpfung in der E-Mail mit der Einladung, oder sie geben den Konferenz-URL direkt in den Webbrowser ein.

---

4. Klicken Sie auf die Registerkarte **Meetings**.
5. Geben Sie im Bereich **Meeting Options** die Zugriffsebene an, die Benutzern gewährt werden soll:
   - **Allow user to join meetings**. Bei Auswahl dieser Option können Konferenzen nicht erstellt oder geplant werden, Benutzer können jedoch weiter auf die Seite **Meetings** zugreifen, um den Konferenzen beizutreten, zu denen sie eingeladen sind.
   - **Allow user to create and join meetings**. Bei Auswahl dieser Option können Benutzer Konferenzen erstellen, planen und über die Seite **Meetings** darauf zugreifen.
6. Geben Sie die **Authentication Requirements** an, die Benutzer auf von ihnen erstellte Konferenzen anwenden sollen:
   - **Meeting password optional (more accessible)**. Bei Auswahl dieser Option wird dem Ersteller der Konferenz die Entscheidung darüber überlassen, ob für die Teilnahme an der Konferenz ein Kennwort erforderlich ist. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort (sofern vorhanden) kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
   - **Require meeting password (more secure)**. Bei Auswahl dieser Option muss der Ersteller der Konferenz entweder ein Kennwort für die Konferenz erstellen oder das von Secure Meeting erzeugte Kennwort verwenden. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
   - **Require server-generated password (even more secure)** Bei Auswahl dieser Option muss der Ersteller der Konferenz das von Secure Meeting erzeugte Kennwort verwenden. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
   - **Require secure gateway authentication (most secure)**. Bei Auswahl dieser Option können nur solche eingeladene Benutzer an Konferenzen teilnehmen, die am sicheren IVE-Gateway authentifiziert wurden. Wenn Sie diese Option auswählen, muss der Ersteller der Konferenz kein Kennwort für die Konferenz erstellen, da sich alle Benutzer am sicheren IVE-Gateway authentifizieren müssen.

7. Geben Sie die Methode für **Password Distribution** an, die von den Erstellern von Konferenzen angewendet werden soll:
   - Legen Sie **Do not display the password in the notification email (more secure)** fest, damit Ersteller von Konferenzen das Meeting-kennwort manuell an die eingeladenen Teilnehmer verteilen (und nicht automatisch mit der von Secure Meeting versendeten E-Mail-Benachrichtigung). Wenn das Kennwort nicht in der Konferenz-E-Mail enthalten ist, erhöht dies die Sicherheit für die Konferenz.
   - **Display the password in the notification email (more accessible)**, wenn das Konferenz-Kennwort automatisch in der E-Mail-Benachrichtigung verteilt werden soll, die von Secure Meeting gesendet wird.
   - **Allow the meeting creator to decide**, um dem Ersteller der Konferenz zu ermöglichen, festzulegen, ob das Konferenzkennwort mit der automatisch von Secure Meeting versendeten E-Mail-Benachrichtigung verteilt werden soll.
8. Geben Sie an, ob Sie Vorführenden der Konferenz ermöglichen möchten, die Steuerung ihrer Desktops und Anwendungen mit anderen Teilnehmern der Konferenz zu teilen, indem Sie im Bereich **Remote Control** eine der folgenden Optionen auswählen:
   - **Allow remote control of shared windows (more functional)**. Die Auswahl dieser Option erlaubt dem Vorführenden oder Leiter der Konferenz, die Steuerung des Desktops und der Desktop-anwendungen des Vorführenden an einen beliebigen Teilnehmer der Konferenz abzugeben, nicht nur an IVE-Benutzer.
   - **Disable remote control (more secure)**. Die Auswahl dieser Option beschränkt die Steuerung des Desktops und der Desktop-anwendungen des Vorführenden der Konferenz ausschließlich auf den Vorführenden selbst.
9. Geben Sie im Bereich **Meeting Policy Settings** an, ob Sie die von Secure Meeting-Benutzern verwendeten Ressourcen einschränken möchten:
   - Aktivieren Sie das Kontrollkästchen **Limit number of simultaneous meetings**, und geben Sie einen entsprechenden Wert für die Höchstanzahl von Konferenzen ein, die gleichzeitig von Mitgliedern der Rolle abgehalten werden kann.
   - Aktivieren Sie das Kontrollkästchen **Limit number of simultaneous meeting attendees**, und geben Sie einen entsprechenden Wert für die Höchstanzahl von Personen ein, die gleichzeitig an von Mitgliedern der Rolle geplanten Konferenzen teilnehmen können.

- Aktivieren Sie das Kontrollkästchen **Limit duration of meetings (minutes)**, und geben Sie einen entsprechenden Wert (in Minuten) für die maximale Dauer einer Konferenz ein.

Wichtig: Das IVE begrenzt die Anzahl von Konferenzen, an denen Benutzer teilnehmen können. Ein einzelner Benutzer kann pro Computer stets nur an einer Konferenz und innerhalb von jeweils 3 Minuten an höchstens 10 aufeinander folgenden Konferenzen teilnehmen. Diese Begrenzungen werden zusätzlich zu den Konferenz- und Benutzerbegrenzungen angewendet, die in Ihrer Secure Meeting-Lizenz festgelegt sind.

---

10. Klicken Sie auf **Save Changes**. Das IVE fügt auf den Startseiten von sicheren Gateways für Benutzer mit der festgelegten Rolle eine Verknüpfung mit der Bezeichnung **Meeting** hinzu.

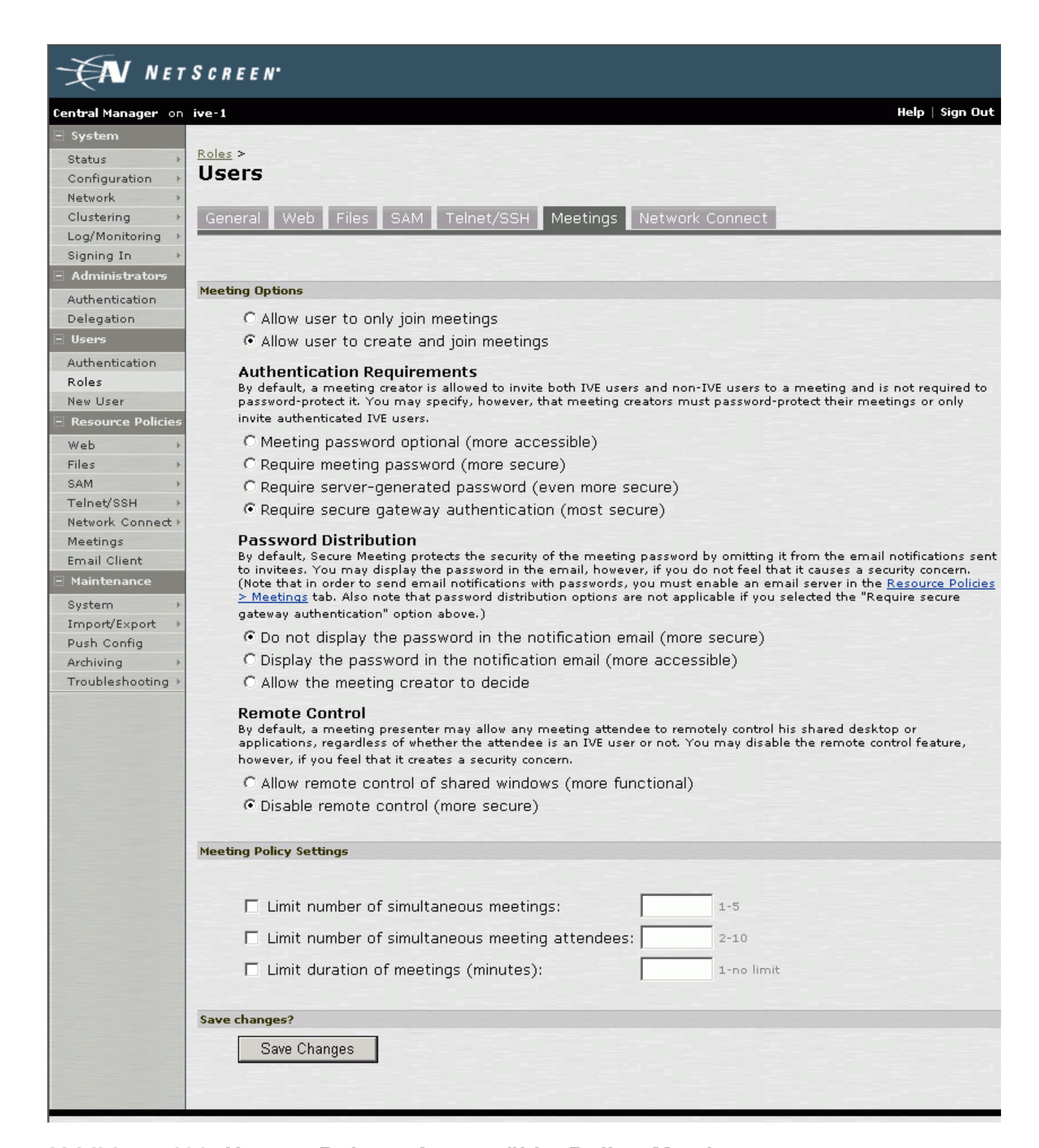


Abbildung 136: Users > Roles > *Ausgewählte Rolle* > Meetings

Registerkarte „Network Connect“

Auf der Registerkarte Network Connect können Sie Optionen für das Teilen von Tunneln und das automatische Starten für eine Rolle angeben.

☑ Angeben von Network Connect-Optionen für das Teilen von Tunneln und das automatische Starten

So geben Sie Network Connect-Optionen für das Teilen von Tunneln und das automatische Starten an:

1. Wählen Sie in der Webkonsole **Users > Roles > *Ausgewählte Rolle* > Network Connect** aus.
2. Wählen Sie unter **Split Tunneling Modes** eine der folgenden Optionen aus:
   - **Disable Split Tunneling** – Der gesamte Netzwerkverkehr des Clients erfolgt über den Network Connect-Tunnel. Wenn durch Network Connect erfolgreich eine Verbindung mit dem IVE hergestellt wird, werden durch das IVE alle vordefinierten lokalen Subnetzrouten und von Host zu Host verlaufende Routen entfernt, die zum Verhalten der Tunnelteilung führen könnten. Wenn die lokale Routingtabelle während einer aktiven Network Connect-Sitzung geändert wird, wird die Sitzung vom IVE beendet.
   - **Allow access to local subnet** – Das IVE behält die lokale Subnetzroute auf dem Client bei, sodass der Zugriff auf lokale Ressourcen wie Drucker beibehalten wird. Die lokale Routingtabelle kann während der Network Connect-Sitzung geändert werden.
   - **Allow access to local subnet with route change monitor** – Nach Beginn einer Network Connect-Sitzung wird die Sitzung bei Änderungen an der lokalen Routingtabelle beendet. Mit dieser Option wird der Zugriff auf lokale Ressourcen wie Drucker beibehalten.
   - **Enable Split Tunneling** – Für diese Option ist das Angeben der Network Connect-Netzwerke erforderlich, an die der Verkehr über das IVE weitergeleitet werden muss, indem Ressourcenrichtlinien für das Teilen von Tunneln definiert werden (siehe : auf Seite 515). Network Connect ändert Routen auf Clients, damit für die genannten Netzwerke bestimmter Verkehr an Network Connect und jeder weitere Verkehr über den lokalen physischen Adapter geleitet wird. Das IVE versucht, alle DNS-Anforderungen zunächst über den physischen Adapter aufzulösen, und leitet anschließend die fehlgeschlagenen Anforderungen an den Network Connect-Adapter weiter.

3. Wählen Sie unter **Auto Launch Options** die Option **Auto-launch Network Connect**, um Network Connect automatisch zu starten, wenn ein authentifizierter Benutzer einer oder mehreren Rollen zugeordnet ist, die Network Connect aktivieren.
4. Klicken Sie auf **Save Changes**.

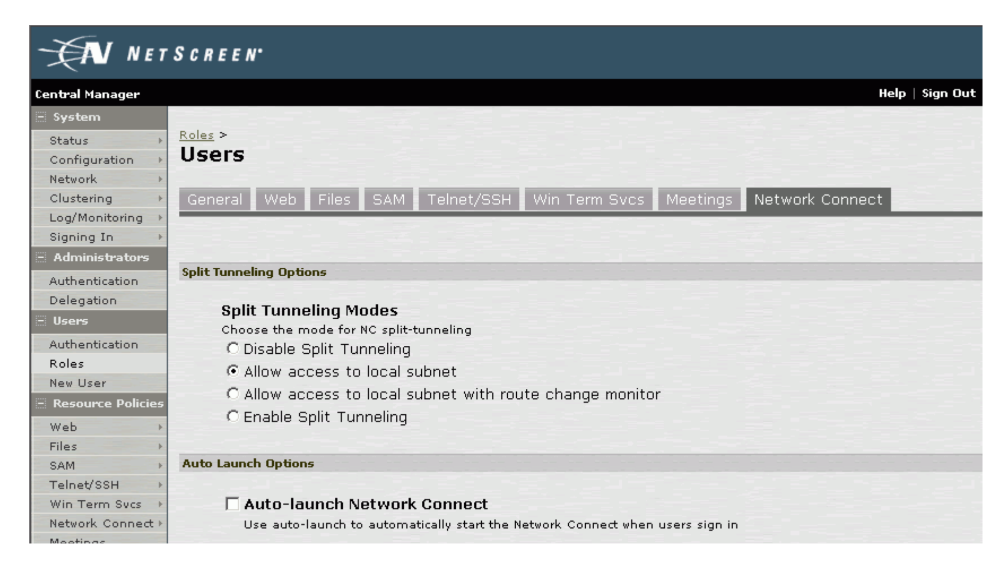


Abbildung 137: **Users > Roles > *Ausgewählte Rolle* > Network Connect**

Konfigurieren der Seite „New User“

☑ Erstellen **lokaler Benutzer**

Wenn Sie als Typ des Authentifizierungsservers „IVE Authentication“ auswählen, müssen Sie für diese Datenbank Datensätze für lokale Benutzer definieren. Lokale Benutzerdatensätze bestehen aus einem Benutzernamen, dem vollständigen Namen und dem Kennwort des Benutzers. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie schnell eine Gruppe von temporären Benutzern erstellen möchten.

So erstellen Sie lokale Benutzerdatensätze für die lokale IVE-Authentifizierung:

1. Führen Sie in der Webkonsole einen der folgenden Vorgänge aus:
   - Wählen Sie **System > Signing In > Servers** aus, und klicken Sie auf die IVE-Datenbank, der Sie ein Benutzerkonto hinzufügen möchten. Klicken Sie auf die Registerkarte **Users** und dann auf **New**.
   - Wählen Sie **Users > New User** aus.
2. Geben Sie den Benutzernamen, den vollständigen Namen des Benutzers und ein Kennwort ein. Hinweis:
   - In Benutzernamen darf die Zeichenkombination „~~“ nicht enthalten sein.
   - Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto erstellen.
3. (Nur auf der Seite **Users > New User**) Wählen Sie aus der Liste **Authenticate Using** die IVE-Datenbank aus, der Sie ein Benutzerkonto hinzufügen möchten.
4. Klicken Sie auf **Save Changes**. Der Benutzerdatensatz wird der IVE-Datenbank hinzugefügt.

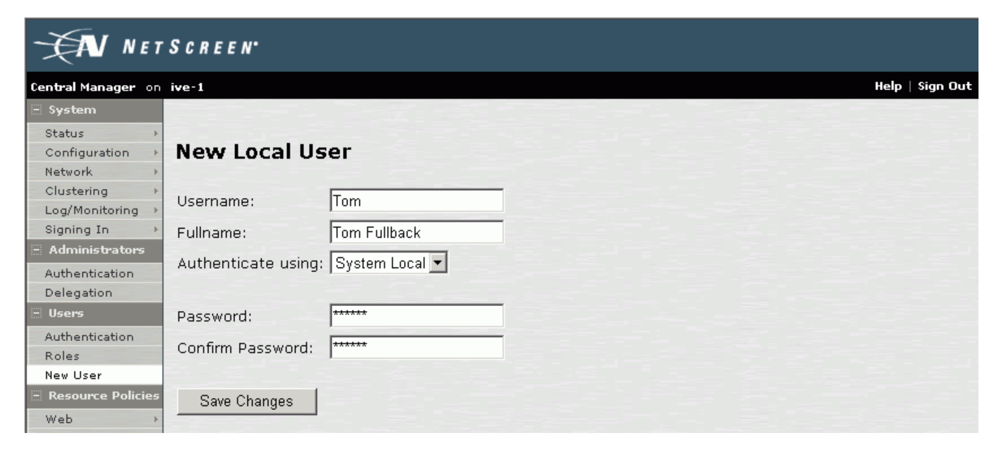


Abbildung 138: **Users > New User**

Konfigurieren der Seite „Web“

Die Seite **Resource Policies > Web** enthält die folgenden Registerkarten:

Auf der Seite **Resource Policies > Web** können Sie Folgendes durchführen:

Schreiben einer Webressourcenrichtlinie

Wenn Sie einer Rolle Zugriff auf das Web gewähren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Ressourcen ein Benutzer zugreifen darf, ob das IVE den vom Benutzer angeforderten Inhalt neu schreiben muss sowie Angaben zu Zwischenspeicherung, zum Applet und zu Anforderungen für die Einzelanmeldung machen. Für jede Webanforderung ermittelt das IVE die konfigurierten[1] Richtlinien für das Neuschreiben. Wenn der Benutzer eine Ressource anfordert, die nicht neu geschrieben werden darf („don't rewrite"), weil sie entweder selektiv neu geschrieben werden soll oder aufgrund einer Ressourcenrichtlinie für Durchgangsproxy, leitet das IVE die Anforderung des Benutzers an die entsprechende Back-End-Ressource weiter. Andernfalls setzt das IVE die Auswertung der Ressourcenrichtlinien fort, die der Anforderung entsprechen, wie z. B. Java-Ressourcenrichtlinien bei der Anforderung eines Java-Applet. Wenn das IVE für eine Benutzeranforderung einer Ressource, die in der entsprechenden Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Webressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Webrichtlinie müssen Sie Webserver oder bestimmte URLs angeben. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46.
- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.
- **Aktionen:** Jeder Typ von Ressourcenrichtlinie führt eine bestimmte Aktion aus: Zugriff auf eine Ressource gewähren bzw. verweigern oder eine Funktion, wie Neuschreiben von Inhalten, Neusignieren von Applets, Bereitstellen von Webdaten ausführen bzw. nicht ausführen. Sie können auch detaillierte Regeln schreiben, mit denen Sie weitere Bedingungen für eine Benutzeranforderung festlegen. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.

1. Wenn Sie kein Neuschreiben von Ressourcenrichtlinien („Rewriting") konfigurieren, setzt das IVE die Auswertung anhand der Richtlinien fort, die für die Anforderung des Benutzers gelten.

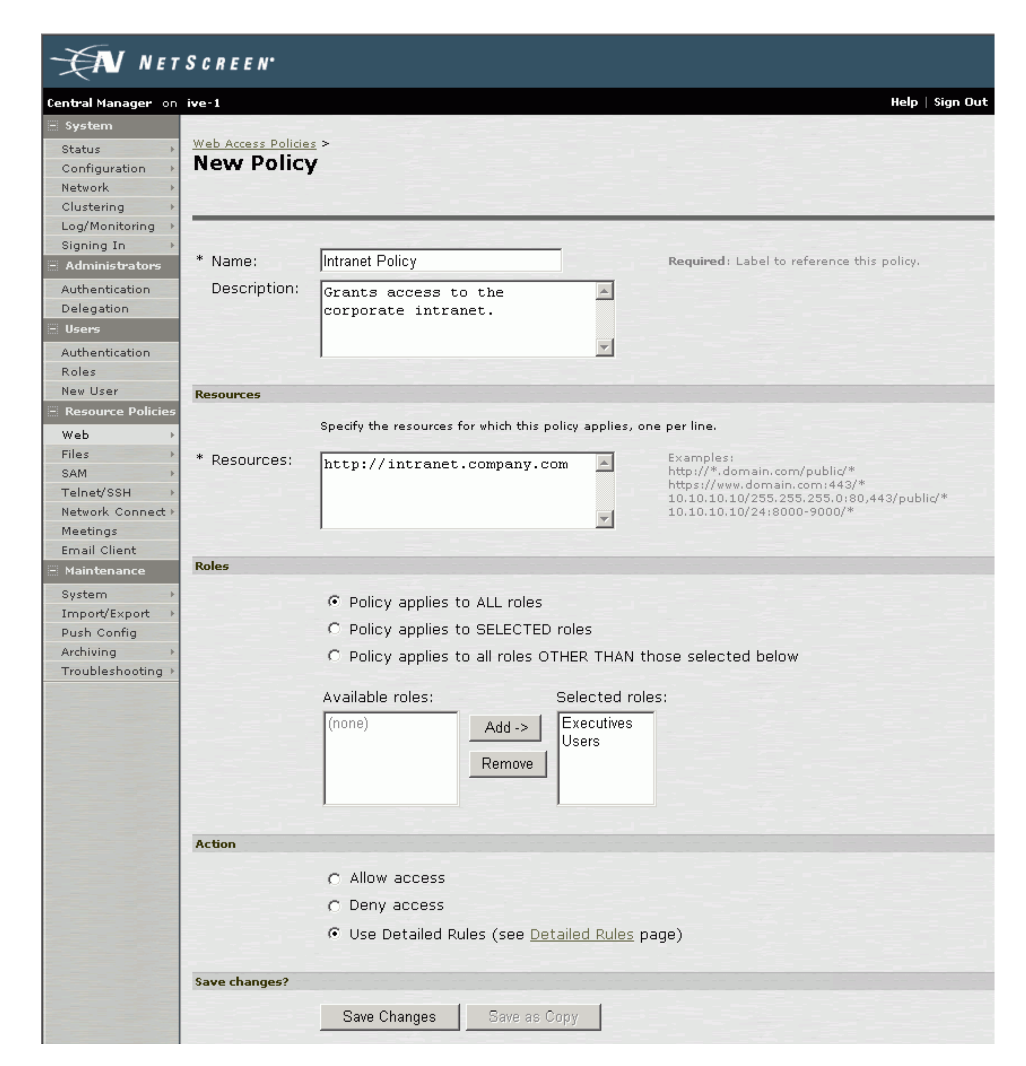


Abbildung 139: Resource Policies > Web > Access > New Policy

Diese Abbildung zeigt eine typische **New Policy**-Konfigurationsseite für eine Webressourcenrichtlinie. Weitere Informationen zum Eingeben der Informationen in die Liste **Resources** finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie" auf Seite 45.

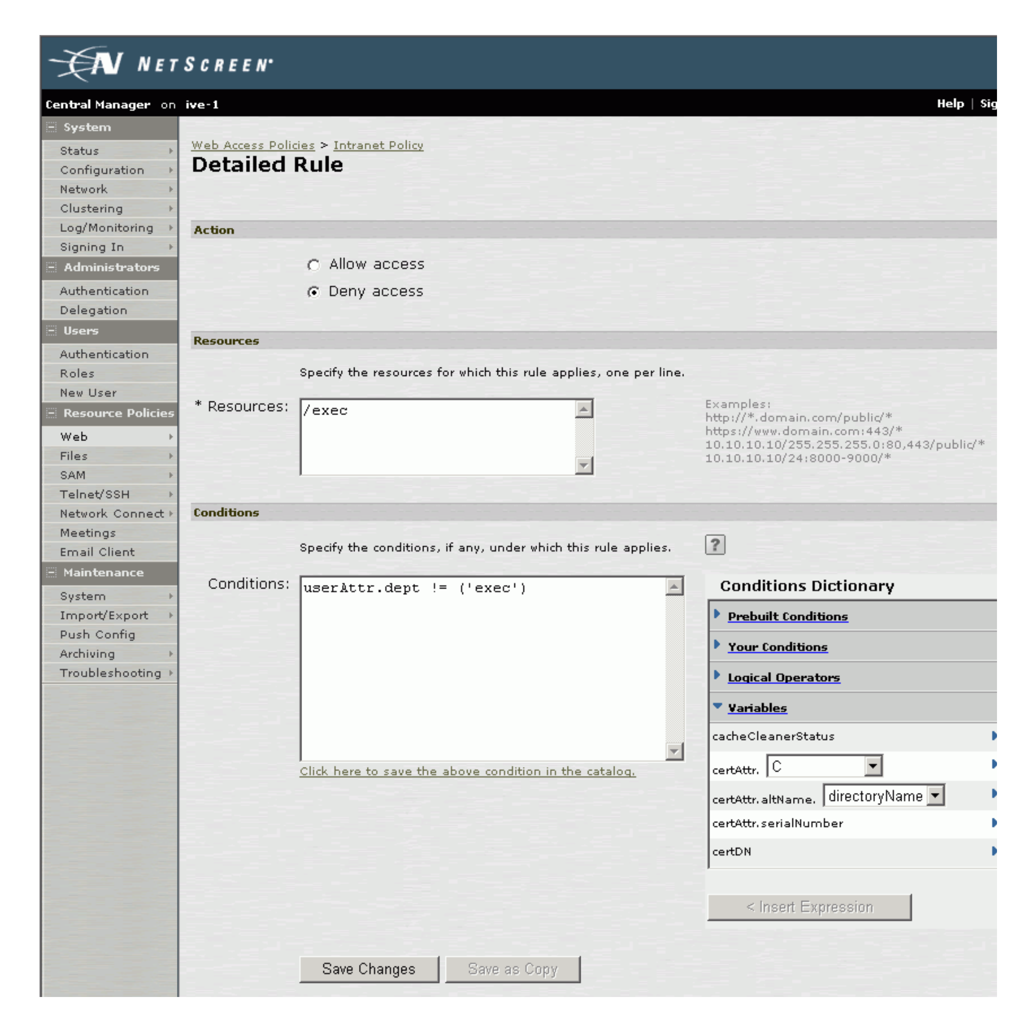


Abbildung 140: Resource Policies > Web > Access > New Policy > Detailed Rule
Diese Abbildung zeigt, wie einer Richtlinie eine detaillierte Regel hinzugefügt wird. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

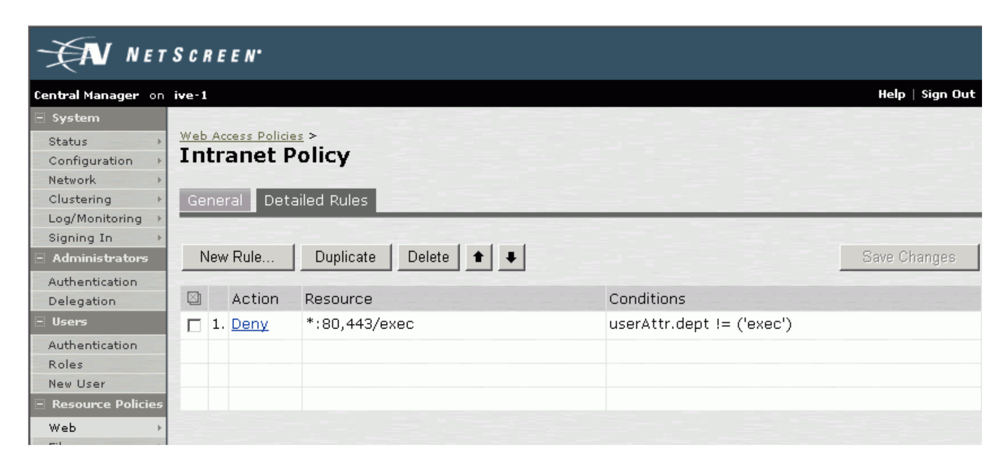


Abbildung 141: **Resource Policies > Web > Access > New Policy > Detailed Rule Added**

Registerkarte „Access“

Auf der Registerkarte **Access** können Sie eine Webressourcenrichtlinie schreiben, die steuert, auf welche Webressourcen Benutzer zugreifen dürfen, um eine Verbindung mit dem Internet, Intranet oder Extranet herzustellen. Sie können den Zugriff auf Webressourcen nach URL oder IP-Bereich zulassen bzw. verweigern. Für URLs können Sie die Platzhalter „*“ und „?“ verwenden, um mehrere Hostnamen und Pfade effektiv anzugeben. Für Ressourcen, die Sie nach Hostnamen angeben, können Sie außerdem entweder HTTP, HTTPS oder beide Protokolle auswählen.

☑ Schreiben einer Ressourcenrichtlinie für den Webzugriff

So schreiben Sie eine Ressourcenrichtlinie für den Webzugriff:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Access** aus.
2. Klicken Sie auf der Seite **Web Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Dies ist optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen" auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Web Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie" auf Seite 443.

Registerkarte „Caching > Policies“

Auf der Registerkarte **Caching > Policies** können Sie eine Webressourcenrichtlinie schreiben, die steuert, welche Webinhalte auf einem Benutzercomputer zwischengespeichert werden. Die Zwischenspeicherung im Browser ist standardmäßig deaktiviert, so dass das IVE sämtliche Seiten, die für Remotebenutzer bereitgestellt werden, als nicht zwischenspeicherungsfähig markiert. Durch diese Einstellung wird verhindert, dass vertrauliche Seiten auf Remotecomputern verbleiben, nachdem ein Benutzer den Browser geschlossen hat. Diese Option kann jedoch auch zu einer Verlangsamung des Browsers führen, weil sie zum wiederholten Abrufen von Inhalten führt. Bei sehr langsamen Verbindungen können Probleme mit der Systemleistung auftreten. Alternativ können Sie eine Richtlinie angeben, die gestattet, dass einige Inhalte wie Bilder, die eine bestimmte Größenbeschränkung nicht überschreiten, zwischengespeichert werden können.

Browserunterstützung

Bei den Cachesteuerungsdirektiven handelt es sich um W3C-Standards, die von allen kompatiblen Browsern unterstützt werden. In der folgenden Liste der von IVE unterstützten Browser werden die Header zur Cachesteuerung berücksichtigt:

- Win2k-IE5.5 SP2
- Win2k-IE 6.0
- Win98-Netscape4.79
- Win98-IE5.5, SP2
- MacOS9.2-IE5.1.5
- MacOSx-IE 5.2

☑ Schreiben einer Ressourcenrichtlinien für die Zwischenspeicherung

So schreiben Sie eine Ressourcenrichtlinie für die Webzwischenspeicherung:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Caching > Policies** aus.
2. Klicken Sie auf der Seite **Web Caching Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen" auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Smart Caching** (Headers senden, die für Inhalt und Browser geeignet sind)

     Falls das IVE im „user-agent"-Header „msie" oder „windows-media-player" erkennt und sich die Anforderung auf eine Mediendatei bezieht, sendet das IVE keinen Antwortheader `cache` oder `cache-control:no-store`.

     Beispiel:

```
(wenn in „content type“ das Element „audio/x-pn-realaudio“ steht
ODER
 wenn „content type“ mit „video/“ beginnt ODER
 wenn „content type“ mit „audio/“ beginnt ODER
 wenn „content type“ gleich „application/octet-stream“ ist und
die
  Dateierweiterung mit „rm“ oder „ram“ beginnt
)
```

In diesen Fällen entfernt das IVE den `cache-control`-Header des Ursprungsservers, und der Inhalt kann zwischengespeichert werden. Durch dieses Verhalten können Mediendateien ordnungsgemäß funktionieren.

Wenn das IVE im Benutzer-Agent-Header „msie" oder „windows-media-player" erkennt

- und sich die Anforderung auf Flash-Dateien, XLS-, PPS- und PPT-Dateien bezieht,
- und der „Content-Type" application/, text/rtf, text/xml, model/ ist oder
- wenn der Ursprungsserver einen „Content-Disposition"-Header sendet,

sendet das IVE den `cache-control:no-store`-Header und entfernt den Cachesteuerungs-Header des Ursprungsservers.

In allen anderen Fällen fügt das IVE die Antwortheader `pragma:no-cache` oder `cache-control:no-store` hinzu.

Hinweis: ICA-Dateien von Citrix und QuickPlace-Dateien werden anders behandelt. ICA-Dateien von Citrix sind immer zwischenspeicherungsfähig und erhalten auch den Header „cache-control-private". QuickPlace-Dateien, die keiner festgelegten Regel (die Vorrang hat) entsprechen, erhalten die Header CCNS und „cache-control:private".

- **Don't Cache** („Cache Control: No-Store" senden)

  Das IVE entfernt die Cachesteuerungs-Header des Ursprungsservers und fügt stattdessen einen Antwortheader vom Typ `cache-control: no-store` hinzu, falls die vom Browser gesendete User-Agent-Zeichenfolge „msie" oder „windows-media-player" enthält.

- **Don't Cache** („Pragma: No Cache" senden)

  Das IVE fügt der Antwort Header vom Typ `pragma:no-cache` und `cache-control:no-cache` hinzu. Darüber hinaus leitet das IVE die Cacheheader des Ursprungsservers (beispielsweise `age`, `date`, `etag`, `last-modified`, `expires`) nicht weiter.

- **Cache** (Cacheheader nicht hinzufügen/ändern)

  Das IVE fügt keine Antwortheader „pragma:nocache" oder „cachecontrol:nostore" hinzu und leitet die Cacheheader des Ursprungsservers weiter.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.

7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Web Caching Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie" auf Seite 443.

Registerkarte „Caching > Options“

Auf der Registerkarte **Caching > Options** können Sie die maximale Größe einer Bilddatei angeben, die auf einem Client zwischengespeichert werden kann. Wenn der „Content-Type"-Header des Ursprungsservers mit „image/" beginnt und der „Content-Length"-Header eine Größe unter der angibt, die in dieser Option als maximale Größe konfiguriert ist, leitet das IVE die Cacheheader des Ursprungsservers weiter. Andernfalls behandelt das IVE die Anforderung wie bei deaktivierter Zwischenspeicherung.

☑ Angeben von Zwischenspeicheroptionen

So geben Sie Zwischenspeicheroptionen an:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Caching > Options** aus.
2. Klicken Sie auf der Seite **Caching Policies** auf **New Policy**.
3. Klicken Sie auf **Save Changes**.

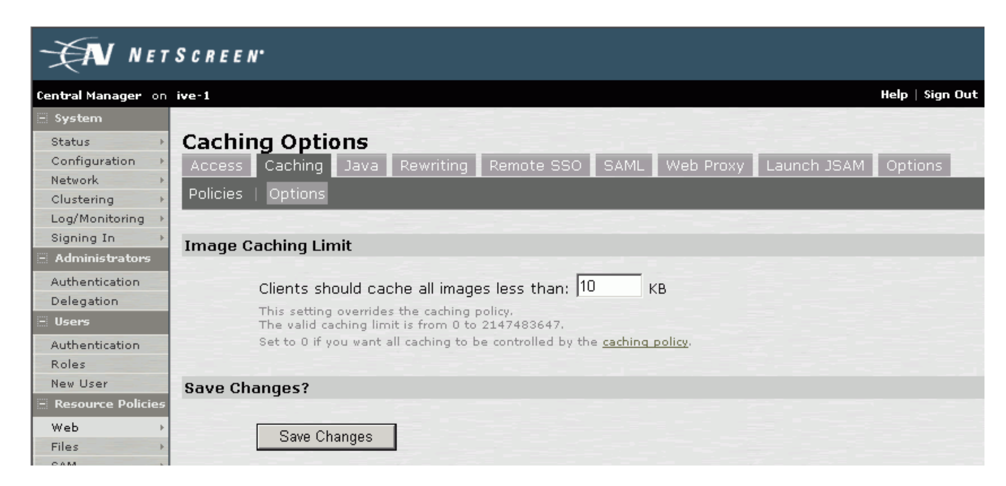


Abbildung 142: **Resource Policies > Web > Caching > Options**

Registerkarte „Java > Access Control“

Auf der Registerkarte **Java > Access Control** können Sie eine Webressourcenrichtlinie schreiben, die steuert, mit welchen Servern und Ports Java-Applets eine Verbindung herstellen können.

☑ Schreiben einer Ressourcenrichtlinie für die Java-Zugriffsteuerung

So schreiben Sie eine Ressourcenrichtlinie für die Java-Zugriffsteuerung:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Java > Access Control** aus.
2. Klicken Sie auf der Seite **Java Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow socket access**

     Erlaubt, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Deny socket access**

     Verhindert, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Java Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie" auf Seite 443.

Registerkarte „Java > Code Signing"

Auf der Registerkarte **Java > Code Signing** können Sie eine Webressourcenrichtlinie schreiben, die angibt, wie das IVE Java-Applets neu schreibt. Wenn das IVE ein signiertes Java-Applet vermittelt, signiert es das Applet standardmäßig mit einem eigenen Zertifikat neu, das nicht mit einem Standardstammzertifikat verkettet ist. Wenn ein Benutzer ein Applet anfordert, das Aufgaben mit einem hohen Risikopotential durchführt, z. B. Zugreifen auf Netzwerkserver, wird im Browser des Benutzers in einer Sicherheitswarnung angezeigt, dass der Stamm nicht vertrauenswürdig ist. Um die Anzeige dieser Warnung zu vermeiden, können Sie ein Codesignaturzertifikat importieren, mit dem das IVE zu vermittelnde Applets neu signiert. Weitere Informationen zu Codesignaturzertifikaten finden Sie unter „Appletzertifikate" auf Seite 72.

Geben Sie beim Konfigurieren der Registerkarte **Applet Certificates** die Server ein, deren Applets Sie als vertrauenswürdig einstufen möchten. Sie können die IP-Adresse oder den Domänennamen eines Servers eingeben. Das IVE signiert nur Applets neu, die von vertrauenswürdigen Servern stammen. Wenn ein Benutzer ein Applet anfordert, das von einem nicht in der Liste aufgeführten Server stammt, verwendet das IVE nicht die importierten Produktionszertifikate zum Signieren des Applets. Dies bedeutet, dass dem Benutzer im Browser eine Sicherheitswarnung angezeigt wird. Für Benutzer der Sun JVM überprüft das IVE außerdem, ob die Stammzertifizierungsstelle des ursprünglichen Appletzertifikats in der Liste vertrauenswürdiger Stammzertifizierungsstellen aufgeführt ist.

☑ Schreiben einer Ressourcenrichtlinie für die Java-Codesignatur

So schreiben Sie eine Ressourcenrichtlinie für die Java-Codesignatur:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Java > Access Control** aus.
2. Klicken Sie auf der Seite **Java Signing Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen" auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Resign applets using applet certificate**

     Erlaubt, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Resign applets using applet certificate**

     Verhindert, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Java Signing Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 443.

Registerkarte „Rewriting > Selective Rewriting“

Auf der Registerkarte **Rewriting > Selective Rewriting** können Sie eine Webressourcenrichtlinie schreiben, die es Ihnen ermöglicht, eine Liste von Hosts festzulegen, für die das IVE Inhalt und Ausnahmen von der Liste vermittelt. Standardmäßig vermittelt das IVE alle Benutzeranforderungen für Webhosts, sofern Sie nicht die Anforderungsverarbeitung für bestimmte Hosts anhand eines anderen Verfahrens konfiguriert haben, z. B. Secure Application Manager.

Erstellen Sie eine Richtlinie für das selektive Neuschreiben, wenn das IVE den Datenverkehr von Websites vermitteln soll, die sich außerhalb des Firmennetzwerks befinden, z. B. „yahoo.com“, oder wenn das IVE keinen Datenverkehr für Client-/Serveranwendungen vermitteln soll, die Sie als Webressourcen bereitgestellt haben, z. B. Microsoft OWA (Outlook Web Access).

☑ Schreiben einer Ressourcenrichtlinie für selektives Neuschreiben

So schreiben Sie eine Ressourcenrichtlinie für selektives Neuschreiben:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Rewriting > Selective Rewriting** aus.
2. Klicken Sie auf der Seite **Web Rewriting Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen" auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Rewrite content**

     Das IVE vermittelt sämtliche Webinhalte der Ressourcen, die in der Liste **Resources** angegeben sind.
   - **Don't rewrite content**

     Das IVE vermittelt keine Webinhalte der Ressourcen, die in der Liste **Resources** angegeben sind. Wenn ein Benutzer eine Ressource anfordert, auf die diese Option zutrifft, zeigt das IVE eine Seite an, die eine Verknüpfung mit der angeforderten Ressource enthält, und der Benutzer wird aufgefordert, auf diese Verknüpfung zu klicken. Über diese Verknüpfung wird die Ressource in einem neuen Browserfenster geöffnet, und die Seite, von der die Anforderung stammt, wird weiterhin im IVE angezeigt.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Web Rewriting Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 443.

Registerkarte „Rewriting > Pass-through Proxy“

Auf der Registerkarte **Rewriting > Pass-through Proxy** können Sie eine Webressourcenrichtlinie schreiben, die Webanwendungen angibt, für die das IVE nur minimale Vermittlung übernimmt. Zum Erstellen einer Ressourcenrichtlinie für Durchgangsproxys müssen Sie zwei Angaben machen:

- Die Webanwendungen, die über den Durchgangsproxy vermittelt werden.
- Die Art der Überwachung von Clientanforderungen an die Anwendungsserver durch das IVE.

Weitere Informationen zu dieser Funktion finden Sie unter „Durchgangsproxy – Übersicht“ auf Seite 111.

☑ Schreiben einer Ressourcenrichtlinie für Durchgangsproxys

So schreiben Sie eine Ressourcenrichtlinie für Durchgangsproxys:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Rewriting > Pass-through Proxy** aus.
2. Klicken Sie auf der Seite **Pass-through Proxy Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)

4. Geben Sie im Feld **URL** einen Hostnamen oder eine IP-Adresse für den Anwendungsserver sowie einen Port an, von dem der URL normalerweise intern auf die Anwendung zugreift.
5. Wählen Sie aus, wie die Durchgangsproxy-Funktion aktiviert werden soll:
   - **Use virtual hostname**

     Wenn Sie diese Option auswählen, müssen Sie einen Hostnamenalias für den Anwendungsserver angeben. Wenn das IVE eine Clientanforderung für den Hostnamenalias des Anwendungsservers empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport im Feld **URL** weiter.

     Wichtig: Wenn Sie diese Option auswählen, müssen Sie auf der Registerkarte **System > Network Settings > Internal Port** im Bereich **Network Identity** auch den IVE-Namen und den Hostnamen definieren.

   - **Use IVE port**

     Wenn Sie diese Option auswählen, müssen Sie einen eindeutigen IVE-Port zwischen 11000-11099 angeben. Das IVE überwacht auf dem angegebenen IVE-Port die Clientanforderungen an den Anwendungs-server und leitet diese an den Anwendungsserverport weiter, der im Feld **URL** angegeben wurde.
6. Geben Sie im Bereich **Action** die Methode an, die das IVE zum Vermitteln des Datenverkehrs verwenden soll:
   - **Rewrite XML**
   - **Rewrite external links**
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Pass-through Proxy Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Anwendung, die von einem Benutzer angefordert wurde, zu einer in der Liste **Resource** angegebenen Anwendung für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.
9. Wenn Sie Folgendes auswählen:
   - **Use virtual hostname**, müssen Sie außerdem Folgendes durchführen:
     1. Hinzufügen einen Eintrags für jeden Hostnamenalias eines Anwendungsservers im externen DNS, der für das IVE aufgelöst wird.
     2. Hochladen eines Serverzertifikats mit Platzhaltern in das IVE (empfohlen).

- **Use IVE port**, müssen Sie Datenverkehr für den IVE-Port öffnen, den Sie für den Anwendungsserver in der Firmenfirewall angegeben haben.

Hinweis: Wenn die Anwendung mehrere Ports überwacht, konfigurieren Sie jeden Anwendungsport als separaten Durchgangsproxyeintrag mit einem separaten IVE-Port. Wenn Sie über verschiedene Hostnamen oder IP-Adressen auf den Server zugreifen möchten, konfigurieren Sie jede dieser Optionen einzeln. In diesem Fall können Sie denselben IVE-Port verwenden.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 443.

Registerkarte „Remote SSO > Form POST“

Auf der Registerkarte **Remote SSO > Form POST** können Sie eine Webressourcenrichtlinie schreiben, die Webanwendungen angibt, an die das IVE Daten sendet. In den Daten können Benutzername und Kennwort eines IVE-Benutzers und durch Systemvariablen gespeicherte Systemdaten enthalten sein. Weitere Informationen zu dieser Funktion finden Sie unter „Remote SSO – Übersicht“ auf Seite 130.

☑ Schreiben einer Ressourcenrichtlinie für Remote-SSO Form POST

So schreiben Sie eine Ressourcenrichtlinie für Remote-SSO Form POST:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Remote SSO > Form POST** aus.
2. Klicken Sie auf der Seite **Form POST Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 479.

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Perform the POST defined below**

     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, führt das IVE mit den Benutzerdaten, die im Bereich **POST details** angegeben sind, einen Form-POST durch.
   - **Do NOT perform the POST defined below**

     Das IVE führt keinen Form-POST mit den Benutzerdaten durch, die im Bereich **POST details** angegeben wurden.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Geben Sie im Bereich **POST details** Folgendes an:
   - URL der Anmeldeseite der Back-End-Webanwendung. Aktivieren Sie **Deny direct login for this resource**, wenn Sie verhindern möchten, dass Benutzer direkt auf diesen URL zugreifen können.
   - Zum Senden bestimmter Benutzerdaten und Änderungsberechtigung für den Benutzer:
     - **User label** – Text, der auf der Benutzerseite **Advanced Preferences** auf dem IVE angezeigt wird. Dieses Feld ist erforderlich, wenn Sie Benutzern erlauben oder von ihnen fordern, Daten zu ändern, die an Back-End-Anwendungen gesendet werden.
     - **Name**– Dieser Name bezeichnet die Daten im Feld **Value**. (Dieser Name wird vermutlich von der Back-End-Anwendung erwartet.)
     - **Value** – Der Wert, der für den angegebenen **Namen** an das Formular gesendet wird. Sie können statische Daten oder eine Systemvariable eingeben. Eine Liste gültiger Variablen finden Sie auf „Systemvariablen und Beispiele“ auf Seite 601.

- **User modifiable?** – Setzen Sie diese Einstellung auf **Not modifiable**, wenn Sie es Benutzern verbieten möchten, Informationen im Feld **Value** zu ändern. Setzen Sie sie auf **User CAN change value**, wenn Sie es dem Benutzer ermöglichen möchten, Daten für eine Back-End-Anwendung anzugeben. Setzen Sie diese Einstellung auf **User MUST change value**, wenn Benutzer zusätzliche Daten eingeben müssen, um auf die Back-End-Anwendung zugreifen zu können. Wenn Sie eine der letzteren Einstellungen auswählen, wird auf der Benutzerseite **Advanced Preferences** auf dem IVE ein Dateneingabefeld angezeigt. Dieses Feld wird mit dem im Feld **User label** eingegebenen Text beschriftet. Wenn Sie im Feld **Value** einen Wert angeben, wird dieser im Feld angezeigt, kann jedoch geändert werden.

8. Klicken Sie auf **Save Changes**.
9. Ordnen Sie die Richtlinien auf der Seite **Form POST Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 443.

Registerkarte „Remote SSO > Headers/Cookies“

Auf der Registerkarte **Remote SSO > Headers/Cookies** können Sie eine Webressourcenrichtlinie schreiben, die benutzerdefinierte Webanwendungen angibt, an die das IVE Header und Cookies sendet. Weitere Informationen zu dieser Funktion finden Sie unter „Remote SSO – Übersicht“ auf Seite 130.

☑ Schreiben einer Ressourcenrichtlinie für SSO-Header und -Cookies

So schreiben Sie eine Ressourcenrichtlinie für SSO-Header/Cookies:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Remote SSO > Headers/Cookies** aus.
2. Klicken Sie auf der Seite the **Headers/Cookies Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
    1. Eine Bezeichnung für diese Richtlinie.
    2. Eine Beschreibung der Richtlinie. (Dies ist optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Append headers as defined below**

     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, sendet das IVE die Benutzerdaten, die im Bereich **POST details** angegeben sind, an den angegebenen URL.
   - **Do NOT append headers as defined below**

     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, sendet das IVE die Benutzerdaten, die im Bereich **POST details** angegeben sind, nicht an den angegebenen URL.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Geben Sie im Bereich **Headers and values** Folgendes an:
   - **Header name** – Text, den das IVE als Headerdaten sendet.
   - **Value** – Wert für den angegebenen Header.
8. Klicken Sie auf **Save Changes**.
9. Ordnen Sie die Richtlinien auf der Seite **Headers/Cookies Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 443.

Registerkarte „SAML > SSO“

Über die Registerkarte **SAML > SSO** können Sie eine Webressourcenrichtlinie schreiben, die SAML-fähige Zugriffsverwaltungssysteme angibt, mit denen das IVE interagiert (wie unter „SAML – Übersicht“ auf Seite 132 beschrieben). Das IVE unterstützt SAML-Einzelanmeldung bei mehreren Assertion Consumer Services, einschließlich von Anwendungen und Domänen. Zum Konfigurieren von SAML SSO-Richtlinien für mehrere Assertion Consumer Services definieren Sie für jede Richtlinie eine eigene Ressourcenrichtlinie.

Dieser Abschnitt enthält die folgenden Anweisungen zum Konfigurieren von SAML SSO-Ressourcenrichtlinien:

☑ Schreiben einer SAML SSO-Artifact-Profil-Ressourcenrichtlinie

Wenn Sie mit dem Artifact-Profil kommunizieren, ruft der vertrauenswürdige Zugriffsverwaltungsserver Authentifizierungsinformationen aus dem IVE ab, wie unter „Artifact-Profil“ auf Seite 135 erklärt.

Wichtig: Wenn Sie das IVE zur Verwendung von Artifact-Profilen konfigurieren, müssen Sie das IVE-Webserverzertifikat für den Assertion Consumer Service installieren (wie unter „Zertifikate“ auf Seite 140 beschrieben).

So schreiben Sie eine SAML SSO-Artifact-Profil-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > SAML > SSO** aus.
2. Klicken Sie auf der Seite **Web Policies** auf **New Policy**.
3. Geben Sie auf der Seite **SAML SSO Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und

Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen" auf Seite 479.

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Use the SAML SSO defined below**

     Das IVE führt eine Einzelanmeldungsanforderung (SSO, Single Sign-On) für den angegebenen URL aus und verwendet dazu die im Bereich **SAML SSO details** angegebenen Daten. Das IVE führt die SSO-Anforderung aus, wenn ein Benutzer versucht, auf eine in der Liste **Resources** angegebene SAML-Ressource zuzugreifen.
   - **Do NOT use SAML**

     Das IVE führt keine SSO-Anforderung durch.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.
7. Geben Sie im Bereich **SAML SSO Details** Folgendes an:
   - **SAML Assertion Consumer Service URL**

     Geben Sie den URL an, den das IVE zum Kontaktieren des Assertion Consumer Service (d. h. des Zugriffsverwaltungsservers) verwenden soll. Beispiel: `https://hostname/acs`. (Beachten Sie, dass das IVE dieses Feld auch verwendet, um den SAML-Empfänger für seine Assertionen zu bestimmen.)

     Wichtig: Wenn Sie einen URL eingeben, der mit „https" beginnt, müssen Sie auf dem IVE die Stammzertifizierungsstelle des Assertion Consumer Service installieren (wie unter „Zertifikate" auf Seite 140 beschrieben).

- **Profile**

  Wählen Sie **Artifact** aus, um anzugeben, dass der Assertion Consumer Service bei SSO-Transaktionen Informationen aus dem IVE abrufen soll.

- **Source ID**

  Geben Sie die Quell-ID für das IVE ein. Geben Sie Folgendes ein, um die entsprechenden Ergebnisse zu erhalten:

  - Klartextzeichenfolge – Wird vom IVE in eine 20-Byte-Zeichenfolge konvertiert, aufgefüllt oder gekürzt.
  - Base-64-codierte Zeichenfolge – Wird vom IVE decodiert und daraufhin überprüft, ob es sich um eine 20-Byte-Zeichenfolge handelt.

  Wenn Ihr Zugriffsverwaltungssystem Base-64-codierte Quell-IDs erfordert, können Sie eine 20-Byte-Zeichenfolge erstellen und diese dann mit einem Tool wie OpenSSL in Base-64-Codierung konvertieren.

  Wichtig: Der IVE-Bezeichner (d. h. die Quell-ID) muss mit dem folgenden URL für den Assertion Consumer Service übereinstimmen (wie unter „Vertrauenswürdige Anwendungs-URLs“ auf Seite 139 erklärt):
  `https://<IVEhostname>/dana-ws/saml.ws`

- **Issuer**

  Geben Sie eine eindeutige Zeichenfolge ein, die vom IVE verwendet werden kann, um sich beim Erstellen von Assertionen selbst zu bezeichnen (normalerweise der eigene Hostname).

  Wichtig: Konfigurieren Sie den Assertion Consumer Service zum Erkennen der eindeutigen Zeichenfolge des IVE (wie unter „Aussteller“ auf Seite 140 beschrieben).

8. Geben Sie im Bereich **User Identity** an, wie das IVE und der Assertion Consumer Service den Benutzer identifizieren sollen:

   - **Subject Name Type**

     Geben Sie an, welche Methode das IVE und der Assertion Consumer Service zum Identifizieren des Benutzers verwenden sollen:

     - **DN** – Senden des Benutzernamens im Format eines DN-Attributs (Distinguished Name).
     - **Email Address** – Senden des Benutzernamens im Format einer E-Mail-Adresse.
     - **Windows** – Senden des Benutzernamens im Format eines qualifizierten Windows-Domänenbenutzernamens.

    - **Other** – Senden des Benutzernamens in einem anderen vom IVE und dem Assertion Consumer Service vereinbarten Format.

- **Subject Name**

  Mit den unter „Systemvariablen und Beispiele" auf Seite 601 beschriebenen Variablen können Sie den Benutzernamen angeben, den das IVE an den Assertion Consumer Service weiterleiten soll. Geben Sie andernfalls statischen Text ein.

  Wichtig: Sie müssen einen Benutzernamen oder ein Attribut senden, der bzw. das vom Assertion Consumer Service erkannt wird (wie unter „Benutzeridentität" auf Seite 144 beschrieben).

9. Geben Sie im Bereich **Web Service Authentication** die Authentifizierungsmethode an, die das IVE zum Authentifizieren des Assertion Consumer Service verwenden soll:
   - **None**

     Der Assertion Consumer Service wird nicht authentifiziert.
   - **Username**

     Der Assertion Consumer Service wird mit einem Benutzernamen und einem Kennwort authentifiziert. Geben Sie den Benutzernamen und das Kennwort ein, die der Assertion Consumer Service an das IVE senden soll.
   - **Certificate Attribute**

     Der Assertion Consumer Service wird mit Zertifikatattributen authentifiziert. Geben Sie die Attribute ein, die der Assertion Consumer Service an das IVE senden soll (ein Attribut pro Zeile). Beispiel: cn=sales. Verwenden Sie Werte, die mit den im Zertifikat des Assertion Consumer Service enthaltenen Werte übereinstimmen.

     Wichtig: Wenn Sie diese Option auswählen, müssen Sie die Stammzertifizierungsstelle des Assertion Consumer Service auf dem IVE installieren (wie unter „Zertifikate" auf Seite 140 erklärt).

10. **Cookie Domain** – Geben Sie eine durch Kommas getrennte Domänenliste ein, an die das SSO-Cookie gesendet wird.
11. Klicken Sie auf **Save Changes**.
12. Ordnen Sie die Richtlinien auf der Seite **SAML SSO Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie" auf Seite 443.

☑ Schreiben einer SAML SSO-POST-Profil-Ressourcenrichtlinie

Wenn Sie mit dem Artifact-Profil kommunizieren, überträgt das IVE Authentifizierungsinformationen an das Zugriffsverwaltungssystem, wie unter „POST-Profil" auf Seite 137 erklärt.

Wichtig: Wenn Sie das IVE zur Verwendung von POST-Profilen konfigurieren, müssen Sie die Stammzertifizierungsstelle des Assertion Consumer Service auf dem IVE installieren und bestimmen, welche Methode der Assertion Consumer Service verwenden soll, um dem Zertifikat zu vertrauen (wie unter „Zertifikate" auf Seite 140 erklärt).

So schreiben Sie eine SAML SSO-POST-Profil-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > SAML > SSO** aus.
2. Klicken Sie auf der Seite **Web Policies** auf **New Policy**.
3. Geben Sie auf der Seite **SAML SSO Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen" auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**
     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**
     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**
     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Use the SAML SSO defined below**

     Das IVE führt eine Einzelanmeldungsanforderung (SSO, Single Sign-On) für den angegebenen URL aus und verwendet dazu die im Bereich **SAML SSO details** angegebenen Daten. Das IVE führt die SSO-Anforderung aus, wenn ein Benutzer versucht, auf eine in der Liste **Resources** angegebene SAML-Ressource zuzugreifen.
   - **Do NOT use SAML**

     Das IVE führt keine SSO-Anforderung durch.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Geben Sie im Bereich **SAML SSO Details** Folgendes an:
   - **SAML Assertion Consumer Service URL**

     Geben Sie den URL an, den das IVE zum Kontaktieren des Assertion Consumer Service (d. h. des Zugriffsverwaltungsservers) verwenden soll. Beispiel: `https://hostname/acs`.
   - **Profile**

     Wählen Sie **POST** aus, um anzugeben, dass das IVE bei SSO-Transaktionen Informationen an den Assertion Consumer Service übergeben soll.
   - **Issuer**

     Geben Sie eine eindeutige Zeichenfolge ein, die vom IVE verwendet werden kann, um sich beim Erstellen von Assertionen selbst zu bezeichnen (normalerweise der eigene Hostname).

     Wichtig: Konfigurieren Sie den Assertion Consumer Service zum Erkennen der eindeutigen Zeichenfolge des IVE (wie unter „Aussteller“ auf Seite 140 beschrieben).

   - **Signing Certificate**

     Geben Sie an, mit welchem Zertifikat das IVE Assertionen signieren soll.
8. Geben Sie im Bereich **User Identity** an, wie das IVE und der Assertion Consumer Service den Benutzer identifizieren sollen:
   - **Subject Name Type**

     Geben Sie an, welche Methode das IVE und der Assertion Consumer Service zum Identifizieren des Benutzers verwenden sollen:
     - **DN** – Senden des Benutzernamens im Format eines DN-Attributs (Distinguished Name).

- **Email Address** – Senden des Benutzernamens im Format einer E-Mail-Adresse.
- **Windows** – Senden des Benutzernamens im Format eines qualifizierten Windows-Domänenbenutzernamens.
- **Other** – Senden des Benutzernamens in einem anderen vom IVE und dem Assertion Consumer Service vereinbarten Format.

- **Subject Name**

  Mit den unter „Systemvariablen und Beispiele" auf Seite 601 beschriebenen Variablen können Sie den Benutzernamen angeben, den das IVE an den Assertion Consumer Service weiterleiten soll. Geben Sie andernfalls statischen Text ein.

Wichtig: Sie müssen einen Benutzernamen oder ein Attribut senden, der bzw. das vom Assertion Consumer Service erkannt wird (wie unter „Benutzeridentität" auf Seite 144 beschrieben).

9. **Cookie Domain** – Geben Sie eine durch Kommas getrennte Domänenliste ein, an die das SSO-Cookie gesendet wird.
10. Klicken Sie auf **Save Changes**.
11. Ordnen Sie die Richtlinien auf der Seite **SAML SSO Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie" auf Seite 443.

Registerkarte „SAML > Access Control"

Über die Registerkarte **SAML > Access Control** können Sie eine Webressourcenrichtlinie schreiben, die SAML-fähige Zugriffsverwaltungssysteme angibt, mit denen das IVE interagiert. Weitere Informationen zu dieser Funktion finden Sie unter „SAML – Übersicht" auf Seite 132. Das IVE unterstützt SAML-Zugriffssteuerungsautorisierung für mehrere Zugriffsverwaltungssysteme. Zum Konfigurieren von SAML-Zugriffssteuerungsrichtlinien für mehrere Anwendungen definieren Sie jeweils eine separate Ressourcenrichtlinie.

☑ Schreiben einer Ressourcenrichtlinie für die SAML-Zugriffsteuerung

Wenn Sie Zugriffsteuerungstransaktionen aktivieren, fragt das IVE den SAML-Webdienst nach Autorisierungsentscheidungen ab (wie in „Informationen zu Zugriffssteuerungsrichtlinien" auf Seite 138 erklärt).

Wichtig: Wenn Sie das IVE zur Verwendung von Zugriffsteuerungstransaktionen konfigurieren, müssen Sie die Stammzertifizierungsstelle des SAML-Webdienstes auf dem IVE installieren (wie in „Zertifikate" auf Seite 140 erklärt).

So schreiben Sie eine Ressourcenrichtlinie für die SAML-Zugriffsteuerung:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > SAML Access Control** aus.
2. Klicken Sie auf der Seite **SAML Access Control Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen" auf Seite 479.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Use the SAML Access Control checks defined below**

     Das IVE führt eine Zugriffssteuerungsprüfung für den angegebenen URL durch und verwendet dazu die im Bereich **SAML Access Control Details** angegebenen Daten.
   - **Do not use SAML Access**

     Das IVE führt keine Zugriffssteuerungsprüfung durch.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.
7. Geben Sie im Bereich **SAML Access Control Details** Folgendes an:
   - **SAML Web Service URL**

     Geben Sie den URL des SAML-Servers des Zugriffsverwaltungssystems ein. Beispiel: `https://hostname/ws`.
   - **Issuer**

     Geben Sie den Hostnamen des Ausstellers ein, der meist mit dem Hostnamen des Zugriffsverwaltungssystems übereinstimmt.

     Wichtig: Geben Sie eine eindeutige Zeichenfolge ein, anhand derer sich der SAML-Webdienst in Autorisierungsassertionen selbst bezeichnet (wie unter „Aussteller" auf Seite 140 erklärt).
8. Geben Sie im Bereich **User Identity** an, wie das IVE und der SAML-Webdienst den Benutzer identifizieren sollen:
   - **Subject Name Type**

     Geben Sie an, welche Methode das IVE und der SAML-Webdienst zum Identifizieren des Benutzers verwenden sollen:
     - **DN** – Senden des Benutzernamens im Format eines DN-Attributs (Distinguished Name).
     - **Email Address** – Senden des Benutzernamens im Format einer E-Mail-Adresse.
     - **Windows** – Senden des Benutzernamens im Format eines qualifizierten Windows-Domänenbenutzernamens.
     - **Other** – Senden des Benutzernamens in einem anderen vom IVE und dem SAML-Webdienst vereinbarten Format.

- **Subject Name**

  Mit den unter „Systemvariablen und Beispiele“ auf Seite 601 beschriebenen Variablen können Sie den Benutzernamen angeben, den das IVE an den SAML-Webdienst weiterleiten soll. Geben Sie andernfalls statischen Text ein.

  Wichtig: Sie müssen einen Benutzernamen oder ein Attribut senden, der bzw. das vom SAML-Webdienst erkannt wird (wie unter „Benutzeridentität“ auf Seite 144 beschrieben).

  ---

9. Geben Sie im Bereich **Web Service Authentication** die Authentifizierungsmethode an, die der SAML-Webdienst zum Authentifizieren des IVE verwenden soll:

   - **None**

     Das IVE wird nicht authentifiziert.

   - **Username**

     Das IVE wird mit einem Benutzernamen und einem Kennwort authentifiziert. Geben Sie den Benutzernamen und das Kennwort ein, die das IVE an den Webdienst senden muss.

   - **Certificate Attribute**

     Das IVE wird mit einem von einer vertrauenswürdigen Zertifizierungsstelle signierten Zertifikat authentifiziert. Wenn auf dem IVE mehrere Zertifikate installiert sind, wählen Sie in der Dropdownliste aus, welches Zertifikat an den Webdienst gesendet werden soll.

     Wichtig: Wenn Sie diese Option auswählen, müssen Sie Zertifikat des IVE-Webservers auf dem Webserver des Zugriffsverwaltungssystems installieren und bestimmen, welche Methode der SAML-Webdienst verwenden soll, um zu bestimmen, ob das Zertifikat vertrauenswürdig ist (wie unter „Zertifikate“ auf Seite 140 beschrieben).

     ---

10. Geben Sie im Bereich **Options** Folgendes an:

    - **Maximum Cache Time**

      Sie können den Aufwand zum Erstellen einer Autorisierungsentscheidung vermeiden, der immer dann entsteht, wenn der Benutzer den gleichen URL anfordert, indem Sie angeben, dass das IVE die Autorisierungsantworten des Zugriffsverwaltungssystems zwischenspeichern muss. Geben Sie die Dauer (in Sekunden) ein, für die das IVE die Antworten zwischenspeichern soll.

- **Ignore Query Data**

  Wenn ein Benutzer eine Ressource anfordert, sendet das IVE standardmäßig den gesamten URL (einschließlich der Abfrageparameter) für diese Ressource an den SAML-Webdienst und speichert den URL zwischen. Sie können angeben, dass das IVE vor dem Anfordern der Autorisierung oder dem Zwischenspeichern der Autorisierungsantwort die Abfragezeichenfolge aus dem URL entfernen soll.

11. Klicken Sie auf **Save Changes**.
12. Ordnen Sie die Richtlinien auf der Seite **SAML Access Control Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 443.

Registerkarte „Web Proxy > Policies“

Auf der Registerkarte **Web Proxy > Policies** können Sie eine Webressourcenrichtlinie schreiben, die benutzerdefinierte Webanwendungen angibt, an die das IVE Header und Cookies sendet. Weitere Informationen zu dieser Funktion finden Sie unter „Remote SSO – Übersicht“ auf Seite 130.

☑ Schreiben einer Ressourcenrichtlinie für Webproxys

So schreiben Sie eine Ressourcenrichtlinie für Webproxys:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Web Proxy > Policies** aus.
2. Klicken Sie auf der Seite **Web Proxy Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 479.

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**
     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**
     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**
     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Access web resources directly**
     Das IVE vermittelt die Anforderung des Benutzers an einen Back-End-Server und die Antwort des Servers an den Benutzer. Dies gilt für Anforderungen an eine Ressource, die in der Liste **Resources** angegeben ist.
   - **Access web resources through a web proxy**
     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, sendet das IVE die Benutzerdaten, die im Bereich **POST details** angegeben sind, nicht an den angegebenen URL. Wenn Sie diese Option auswählen, müssen Sie in der Dropdownliste einen Webproxyserver angeben. Informationen zum Definieren von Webproxyservern finden Sie unter „Registerkarte „Web Proxy > Servers““ auf Seite 476.
   - **Use Detailed Rules**
     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Headers/Cookies Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 443.

Registerkarte „Web Proxy > Servers“

Sie können alle vom IVE durchgeführten Webanforderungen an einen Webproxy leiten, statt mit dem IVE eine direkte Verbindung mit den Webservern herzustellen. Diese Funktion bietet sich an, wenn Ihre Richtlinien für die Netzwerksicherheit diese Konfiguration erfordern oder wenn Sie zur Leistungssteigerung einen Webproxy mit Zwischenspeicherung verwenden möchten.

Hinweis: Derzeit wird die Authentifizierung über Webproxys vom IVE nicht unterstützt. Wenn Sie die Webproxyfunktion des IVE verwenden möchten, müssen Sie Ihren Webproxy so konfigurieren, dass nicht authentifizierte Benutzer akzeptiert werden.

☑ Angeben von Webproxyservern

Auf der Registerkarte **Web Proxy** können Sie Server für Ressourcenrichtlinien für Webproxys angeben.

So geben Sie Webproxyserver an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > Web Proxy > Servers** aus.
2. Geben Sie unter **Web Proxy Servers** den Namen oder die IP-Adresse des Webproxyservers sowie die Portnummer ein, an der der Proxyserver Daten abfragt, und klicken Sie dann auf **Add**. Wiederholen Sie diesen Schritt, um weitere Webproxyserver anzugeben.

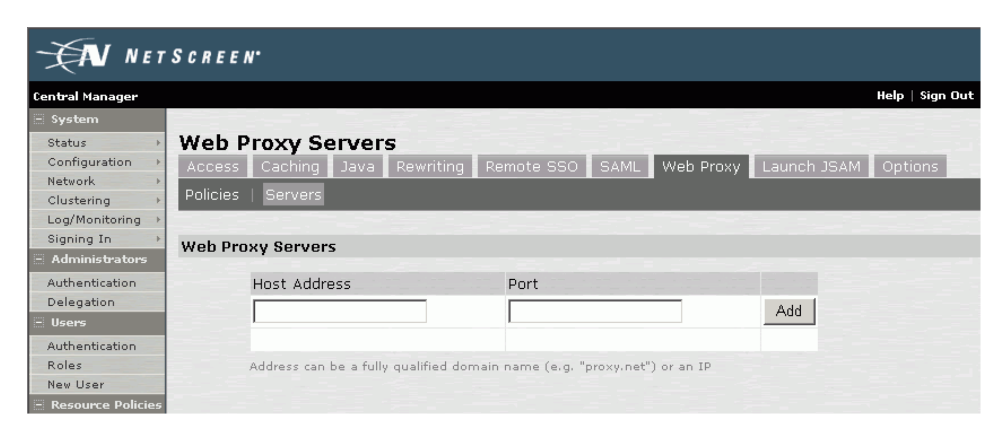


Abbildung 143: **Resource Policies > Web > Web Proxy > Servers**

Registerkarte „Launch JSAM“

Mit der Registerkarte **Launch JSAM** können Sie eine Webressourcenrichtlinie schreiben, die den URL angibt, für den das IVE automatisch J-SAM auf dem Client startet. Das IVE startet das J-SAM in zwei Szenarios:

- Ein Benutzer gibt den URL im Feld **Address** der IVE-Startseite ein.
- Ein Benutzer klickt auf der IVE-Startseite auf ein (von einem Administrator konfigurierten) Weblesezeichen für den URL.

Diese Funktion ist hilfreich, wenn Sie Anwendungen aktivieren, die J-SAM benötigen, aber vermeiden möchten, dass Benutzer J-SAM unnötig ausführen müssen. Diese Funktion erfordert allerdings, dass die Benutzer über die IVE-Startseite auf den URL zugreifen. Wenn die Benutzer den URL im Adressfeld des Browsers eingeben, verarbeitet das IVE die Anforderung nicht.

Wichtig: Das IVE bietet nahtlose Integration mit Citrix. Wenn Sie Citrix als J-SAM-Standardanwendung angeben, startet das IVE automatisch J-SAM, wenn ein Benutzer eine ICA-Datei auswählt. Dies ist sogar dann der Fall, wenn der URL nicht als Ressourcenrichtlinie konfiguriert ist.

☑ Schreiben einer Ressourcenrichtlinie zum Starten von J-SAM

So schreiben Sie eine Ressourcenrichtlinie zum Starten von J-SAM:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > Launch JSAM** aus.
2. Klicken Sie auf der Seite **JSAM Autolaunch Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie (optional).
4. Geben Sie im Bereich **Resources** die URLs an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46. Informationen zum Aktivieren der IP-basierten Zuordnung und der Zuordnung anhand von Groß- und Kleinschreibung für diese Ressourcen finden Sie unter „Angeben von Webressourcenoptionen“ auf Seite 479.

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Launch JSAM for this URL**

     Das IVE lädt den Java-Secure Application Manager auf den Client herunter und bearbeitet dann den angeforderten URL.

     Wichtig: J-SAM wird nur dann automatisch für den angegebenen URL gestartet, wenn ein Benutzer auf der IVE-Startseite den URL eingibt oder ein Lesezeichen für den URL auswählt (**Browsing > Bookmarks**).

   - **Don't Launch JSAM for this URL**

     Das IVE lädt den Java-Secure Application Manager für den angeforderten URL nicht auf den Client herunter. Diese Option ist nützlich, wenn Sie das automatische Starten von J-SAM für die angegebenen URLs vorübergehend deaktivieren möchten.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.

Registerkarte „Options“

Über die Registerkarte **Options** können Sie Webressourcenoptionen festlegen, die auf Ihre Webressourcenrichtlinien anwendbar sind. Folgende Optionen stehen zur Verfügung:

- **IP based matching for Hostname based policy resources** – Das IVE sucht nach IP-Adressen, die den einzelnen in einer Webressourcen-richtlinie angegebenen Hostnamen entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle des Hostnamens angibt, vergleicht das IVE die IP mit zwischengespeicherten Liste von IP-Adressen, um zu bestimmen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

  Hinweis: Diese Option wird nicht auf Hostnamen angewendet, die Platzhalter und Parameter enthalten.

- **Case sensitive matching for the Path and Query string components in Web resources** – Benutzer müssen für eine Ressource einen URL eingeben, bei dem die Groß- und Kleinschreibung berücksichtigt wird. Verwenden Sie diese Option beispielsweise beim Übergeben des Benutznamens oder des Kennwortes in einem URL.

Wenn Sie eine Dateiressourcenrichtlinie aktivieren, kompiliert das IVE eine Liste der Hostnamen, die im Feld **Resources** der jeweiligen Web-ressourcenrichtlinie angegeben sind. Daraufhin wendet das IVE die aktivierten Optionen auf diese umfassende Liste mit Hostnamen an.

☑ Angeben von Webressourcenoptionen

So geben Sie eine Webressourcenoption an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Web > Options** aus.
2. Wählen Sie Folgendes aus:
   - **IP based matching for Hostname based policy resources**
   - **Case sensitive matching for the Path and Query string components in Web resources**
3. Klicken Sie auf **Save Changes**.

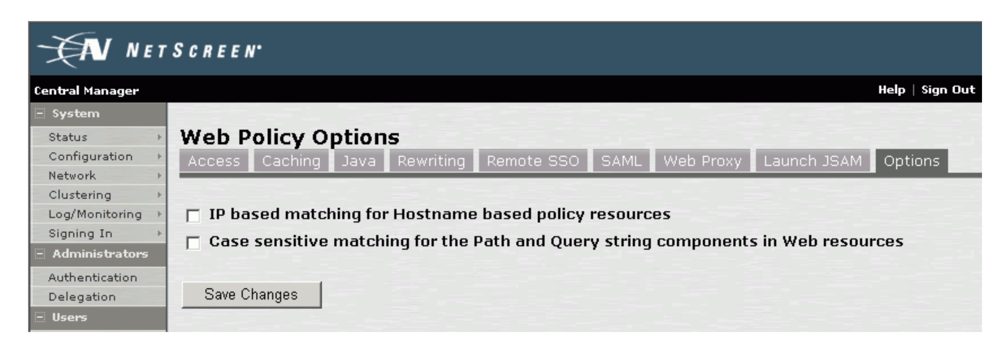


Abbildung 144: **Resource Policies > Web > Options**

Konfigurieren der Seite „Files“

Die Seite **Resource Policies > Files** enthält die folgenden Registerkarten:

Auf der Seite **Resource Policies > Files** können Sie Folgendes durchführen:

Schreiben einer Dateiressourcenrichtlinie

Wenn Sie die Dateizugriffsfunktion für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Windows- und UNIX/NFS-Ressourcen ein Benutzer zugreifen darf und welche Codierung für die Kommunikation mit Windows- und NFS-Dateifreigaben verwendet werden soll. Wenn ein Benutzer eine Datei anfordert, wertet das IVE die entsprechenden Ressourcenrichtlinien aus, z. B. Ressourcenrichtlinien für den Windows-Zugriff bei einer Anforderung eines MS Word-Dokuments (DOC-Datei). Wenn das IVE für eine Benutzeranforderung einer Ressource, die in der entsprechenden Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Dateiressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Dateirichtlinie müssen Sie Dateiserver oder bestimmte Freigaben angeben. Weitere Informationen finden Sie unter „Angeben von Windows-Dateiressourcen“ auf Seite 48 und „Angeben von UNIX/NFS-Dateiressourcen“ auf Seite 49.

- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.
- **Aktionen:** Jeder Typ von Ressourcenrichtlinie führt eine bestimmte Aktion aus: Zugriff auf eine Ressource gewähren bzw. verweigern oder eine Funktion ausführen bzw. nicht ausführen, z. B. einem Benutzer Schreibzugriff auf ein Verzeichnis zu gewähren. Sie können auch detaillierte Regeln schreiben, mit denen Sie weitere Bedingungen für eine Benutzeranforderung festlegen. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

Registerkarte „Windows > Access“

Über die Registerkarte **Windows > Access** können Sie eine Dateiressourcenrichtlinie schreiben, die angibt, auf welche Windows-Ressourcen Benutzer zugreifen dürfen. Für Windows-Ressourcen geben Sie den Server und die Freigabe sowie bei Bedarf den Pfad für einen bestimmten Ordner ein.

☑ Schreiben einer Ressourcenrichtlinie für Windows-Zugriff

So schreiben Sie eine Ressourcenrichtlinie für Windows-Zugriff:

1. Wählen Sie in der Webkonsole **Resource Policies > File > Windows > Access** aus.
2. Klicken Sie auf der Seite **Windows File Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Windows-Dateiressourcen“ auf Seite 48.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

- **Policy applies to all roles OTHER THAN those selected below**

  Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind. Aktivieren Sie **Read-only**, damit die Benutzer keine Dateien auf dem Server speichern können.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Windows File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

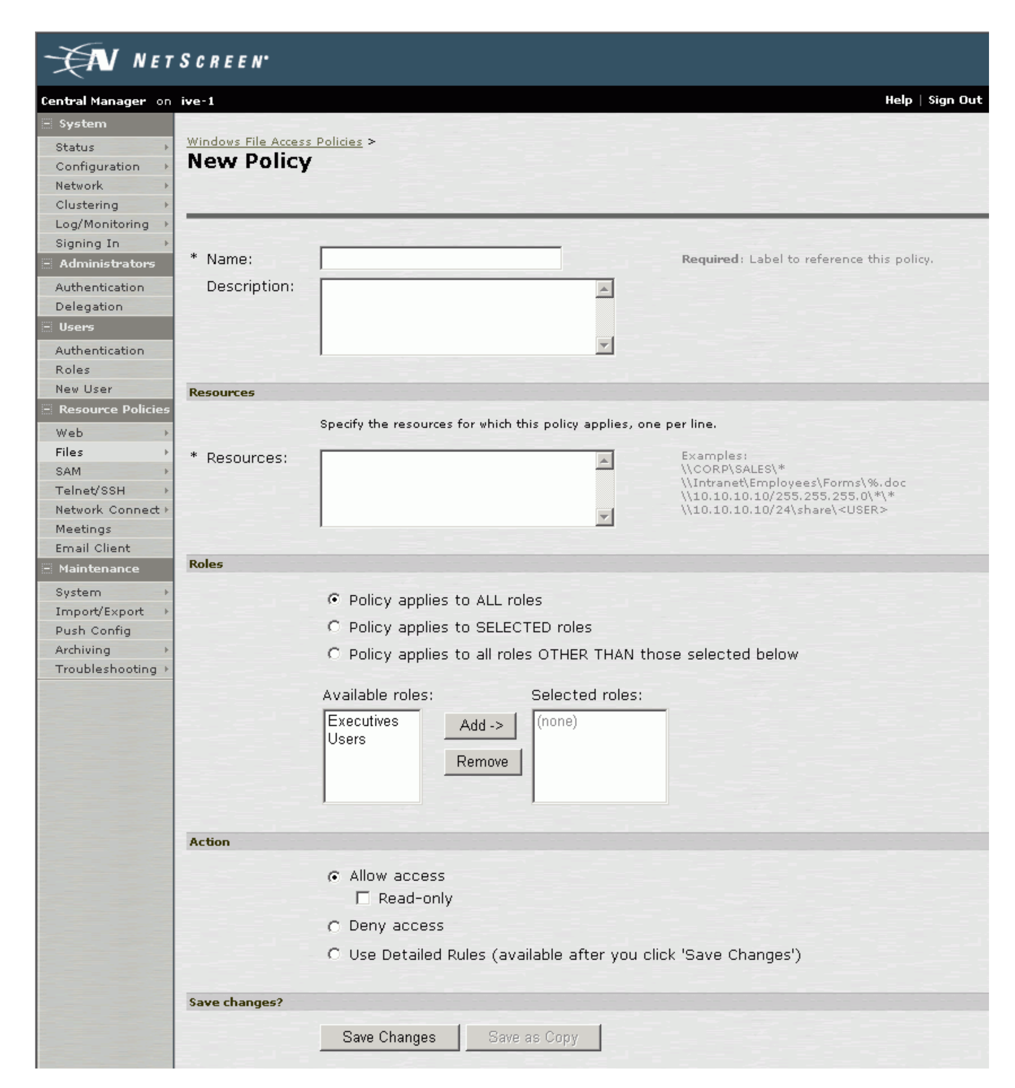


Abbildung 145: **Resource Policies > Files > Windows > Access > New Policy**

Registerkarte „Windows > Credentials“

Auf der Registerkarte **Windows > Credentials** können Sie eine Dateiressourcenrichtlinie schreiben, mit der Sie Anmeldeinformationen für das IVE angeben können, die an einen Dateiserver gesendet werden, wenn eine Benutzeranfrage einer Ressource in der Liste **Resource** entspricht. Sie können außerdem das IVE so konfigurieren, dass Benutzer zur Eingabe ihrer Anmeldeinformationen aufgefordert werden.

☑ Schreiben einer Ressourcenrichtlinie für Windows-Anmeldeinformationen

So schreiben Sie eine Ressourcenrichtlinie für Windows-Anmeldeinformationen:

1. Wählen Sie in der Webkonsole **Resource Policies > File > Windows > Credentials** aus.
2. Klicken Sie auf der Seite **Windows Credentials Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Windows-Dateiressourcen“ auf Seite 48.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Use specified credentials**

     Mithilfe dieser Option können Sie Administrator-Anmeldeinformationen angeben, die das IVE an die Ressourcen sendet, die auf Ordner- und Dateiebene in der Liste **Resources** angegeben ist. Der IVE-Server für die Dateinavigation hält jedoch die Verbindungen mit einem Server\Freigabe offen, sodass die Verbindung mit einem anderen Ordner auf derselben Freigabe über ein anderes Konto möglicherweise nicht zuverlässig funktioniert. Wenn die angegebenen Anmeldeinformationen nicht funktionieren, fordert das IVE den Benutzer auf, die Anmeldeinformationen auf einer zwischengeschalteten Seite einzugeben.
   - **Prompt for user credentials**

     Wenn für eine freigegebene Datei, die in der Liste **Resources** angegeben ist, Anmeldeinformationen erforderlich sind, vermittelt das IVE die Anfrage, indem eine Authentifizierungsanfrage auf dem IVE angezeigt wird. Der Benutzer muss die Anmeldeinformationen für die Freigabe eingeben, auf die er zugreifen möchte.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Windows File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

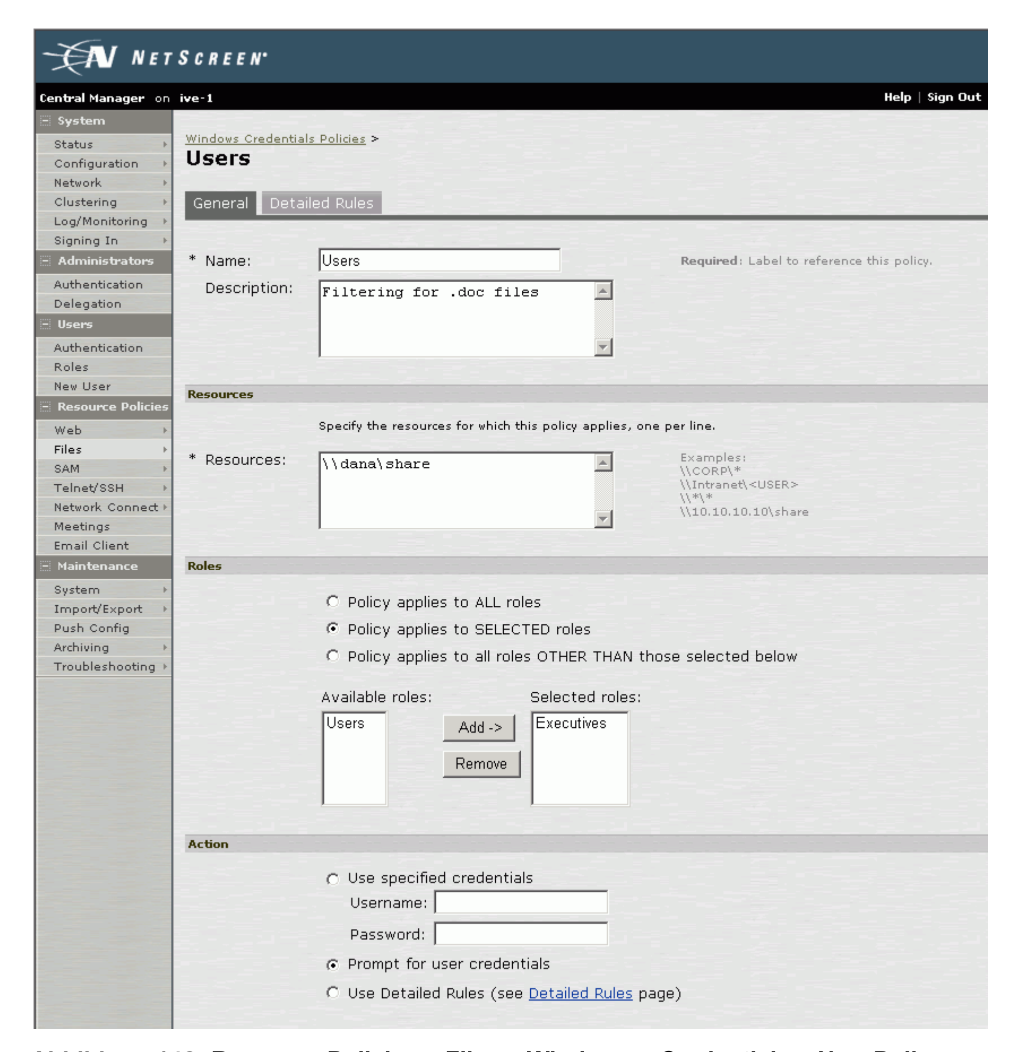


Abbildung 146: **Resource Policies > Files > Windows > Credentials > New Policy**

Registerkarte „UNIX/NFS“

Über die Registerkarte **UNIX/NFS** können Sie eine Dateiressourcenrichtlinie schreiben, die angibt, auf welche UNIX/NFS-Ressourcen Benutzer zugreifen dürfen. Sie geben UNIX/NFS-Ressourcen an, indem Sie einen Serverhostnamen oder die IP-Adresse eingeben und bei Bedarf den Pfad zu einer bestimmten Freigabe angeben.

☑ Schreiben einer UNIX/NFS-Ressourcenrichtlinie

So schreiben Sie eine UNIX/NFS-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole **Resource Policies > File > UNIX/NFS** aus.
2. Klicken Sie auf der Seite **Unix/NFS File Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von UNIX/NFS-Dateiressourcen“ auf Seite 49.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind. Aktivieren Sie **Read-only**, damit die Benutzer keine Dateien auf dem Server speichern können.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Unix/NFS File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

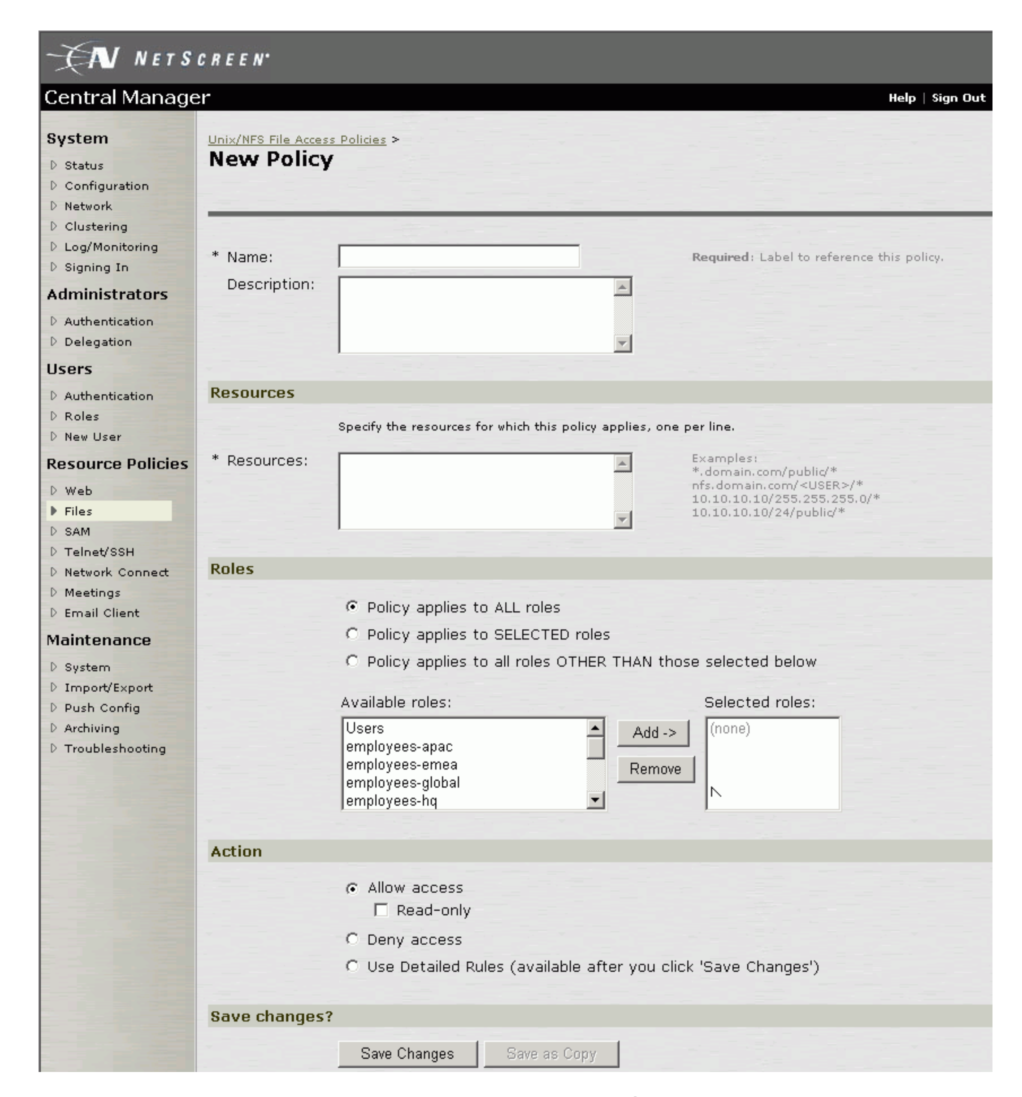


Abbildung 147: Resource Policies > Files > UNIX/NFS > New Policy

Registerkarte „Encoding“

Auf der Registerkarte **Files > Encoding** können Sie festlegen, wie das IVE die Daten bei der Interaktion mit Dateiservern codiert.

☑ Angeben der Codierung für die Internationalisierung von IVE-Datenverkehr

So geben Sie die Codierung für die Internationalisierung von IVE-Datenverkehr an:

1. Wählen Sie in der Webkonsole **Resource Policies > File > Encoding** aus.
2. Wählen Sie die entsprechende Option aus:
   - Western European (ISO-8859-1)
   - Simplified Chinese (CP936)
   - Simplified Chinese (GB2312)
   - Traditional Chinese (CP950)
   - Traditional Chinese (Big5)
   - Japanese (Shift-JIS)
   - Korean
3. Klicken Sie auf **Save Changes**.

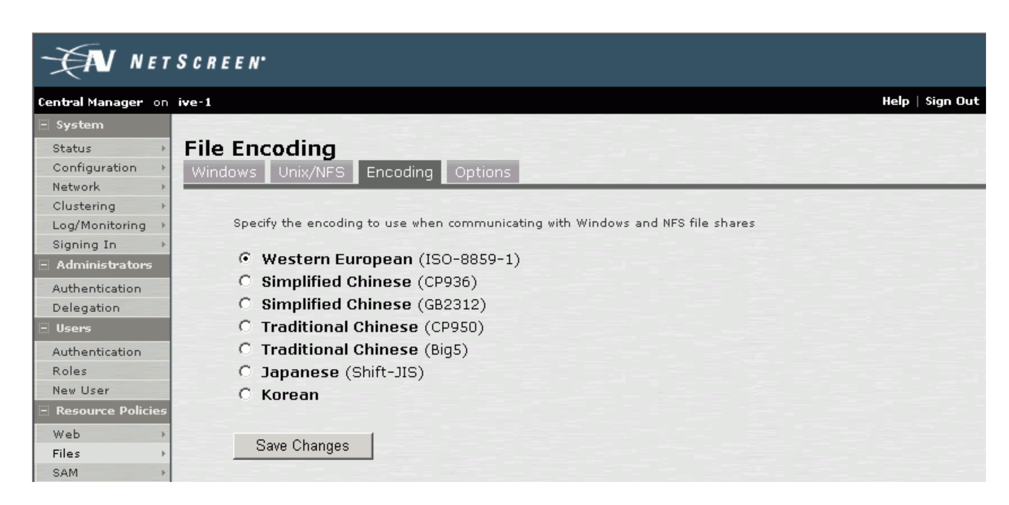


Abbildung 148: **Resource Polices > Files > Encoding**

Registerkarte „Options“

Über die Registerkarte **Options** können Sie Dateiressourcenoptionen festlegen, die auf Ihre Dateiressourcenrichtlinien anwendbar sind. Folgende Optionen stehen zur Verfügung:

- **IP based matching for Hostname based policy resources** – Das IVE sucht nach IP-Adressen, die den einzelnen in einer Dateiressourcen-richtlinie angegebenen Hostnamen entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle des Hostnamens angibt, vergleicht das IVE die IP mit zwischengespeicherten Liste von IP-Adressen, um zu bestimmen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

  Hinweis: Diese Option wird nicht auf Hostnamen angewendet, die Platzhalter und Parameter enthalten.

- **Case sensitive matching for the Path and Query string components in Web resources** – Benutzer müssen für eine Ressource einen URL eingeben, bei dem die Groß- und Kleinschreibung berücksichtigt wird. Verwenden Sie diese Option beim Einfügen des Benutznamens oder des Kennwortes in einen URL.

  Hinweis: Diese Option wird auf Windows-Servern nicht angewendet.

Wenn Sie eine Dateiressourcenrichtlinie aktivieren, kompiliert das IVE eine Liste der Hostnamen, die im Feld **Resources** aller Dateiressourcenrichtlinien angegeben ist. Daraufhin wendet das IVE die aktivierten Optionen auf diese umfassende Liste mit Hostnamen an.

☑ Angeben von Dateiressourcenoptionen

So geben Sie eine Dateiressourcenoption an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > File > Options** aus.
2. Wählen Sie Folgendes aus:
   - **IP based matching for Hostname based policy resources**
   - **Case sensitive matching for the Path and Query string components in Web resources**
3. Klicken Sie auf **Save Changes**.

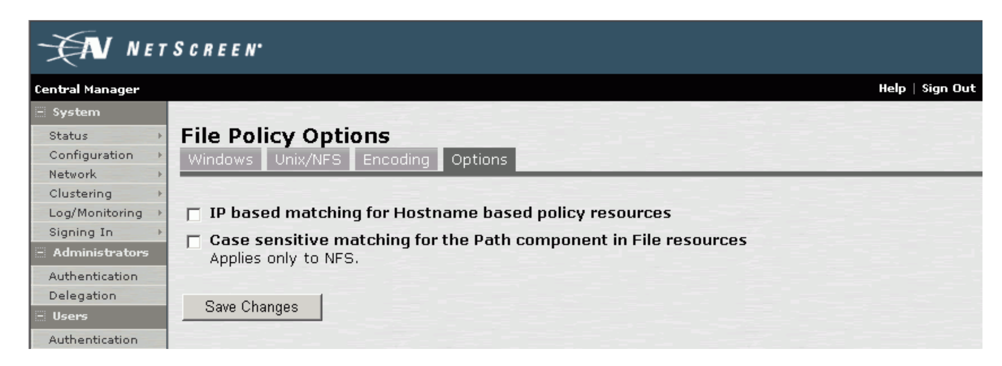


Abbildung 149: **Resource Policies > Files > Options**

Konfigurieren der Seite „SAM“

Die Seite **Resource Policies > SAM** enthält die folgenden Registerkarten:

Über die Registerkarten auf der Seite **Resource Policies > SAM** können Sie Folgendes durchführen:

Mithilfe der Aktualisierungsoption Secure Application Manager können Benutzer über einen verschlüsselten SSL-Tunnel auf Anwendungsserver zugreifen, als ob sie sich im Firmen-LAN befänden. Weitere Informationen finden Sie unter „Secure Application Manager – Übersicht“ auf Seite 115.

Schreiben einer SAM-Ressourcenrichtlinie

Wenn Sie die Zugriffsfunktion Secure Application Manager für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die die Anwendungsserver angeben, auf die die Benutzer zugreifen dürfen. Diese Richtlinien gelten sowohl für die Java- als auch für die Windows-Version von Secure Application Manager (J-SAM bzw. W-SAM). Wenn ein Benutzer eine Anforderung für einen Anwendungsserver vornimmt, wertet das IVE die SAM-Ressourcenrichtlinien aus. Wenn das IVE für eine Benutzeranforderung für eine Ressource, die in einer SAM-Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer SAM-Ressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer SAM-Richtlinie müssen Sie Anwendungsserver angeben, mit denen Benutzer eine Verbindung herstellen können.
- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen. SAM-Ressourcenrichtlinien gelten für alle Benutzeranforderungen, die anhand der Versionen J-SAM oder W-SAM vorgenommen wurden.
- **Aktionen:** Eine Ressourcenrichtlinie für Secure Application Manager erlaubt oder verweigert den Zugriff auf einen Anwendungsserver.

Registerkarte „Access“

Über die Registerkarte **Access** können Sie eine Secure Application Manager-Ressourcenrichtlinie schreiben, die angibt, auf welche Anwendungsressourcen Benutzer zugreifen können.

☑ Schreiben einer Secure Application Manager-Ressourcenrichtlinie

So schreiben Sie eine Secure Application Manager-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > SAM > Access** aus.
2. Klicken Sie auf der Seite **Secure Application Manager Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie (optional).
4. Geben Sie im Bereich **Resources** die Anwendungsserver an, für die diese Richtlinie gelten soll.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow socket access**

     Hiermit erlauben Sie den Zugriff auf die Anwendungsserver, die in der Liste **Resources** aufgeführt sind.
   - **Deny socket access**

     Hiermit verweigern Sie den Zugriff auf die Anwendungsserver, die in der Liste **Resources** aufgeführt sind.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Secure Application Manager Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

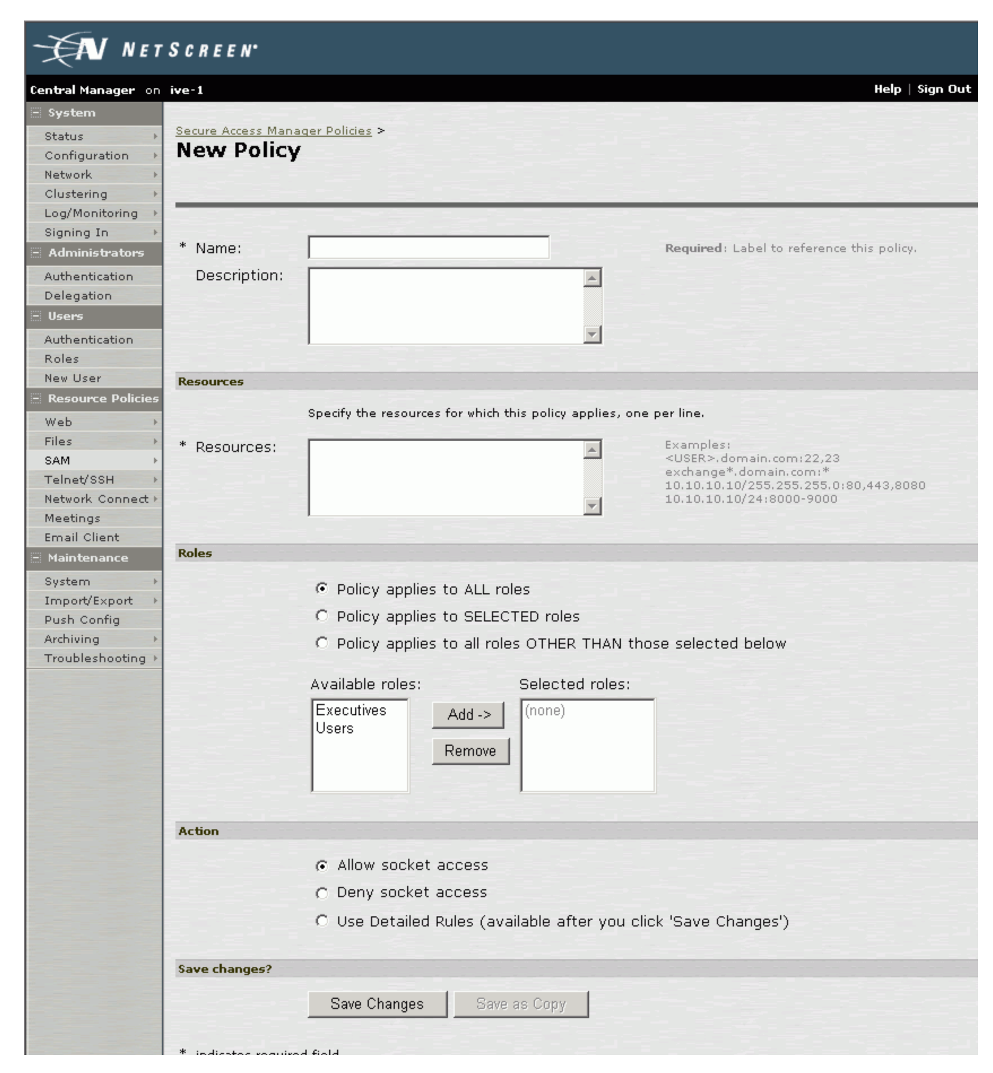


Abbildung 150: Resource Policies > SAM > Access > New Policy

Registerkarte „Options“

Über die Registerkarte **Options** können Sie die SAM-Ressourcenoption so festlegen, dass IP-Adressen mit Hostnamen abgeglichen werden, die in Ihren SAM-Ressourcenrichtlinien als Ressourcen angegeben sind. Wenn Sie diese Option aktivieren, sucht das IVE nach IP-Adressen, die einzelnen in einer SAM-Ressourcenrichtlinie angegebenen Hostnamen entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle eines Hostnamens angibt, vergleicht das IVE die IP mit den IP-Adressen seiner zwischengespeicherten Liste, um zu bestimmen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

Wenn Sie diese Option aktivieren, stellt das IVE eine Liste mit Hostnamen zusammen, die in den Ressourcenfeldern der einzelnen SAM-Ressourcenrichtlinien angegeben sind. Daraufhin wendet das IVE die Option auf diese umfassende Liste mit Hostnamen an.

Hinweis: Diese Option wird nicht auf Hostnamen angewendet, die Platzhalter und Parameter enthalten.

☑ Angeben der SAM-Ressourcenoption

So geben Sie die SAM-Ressourcenoption an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > SAM > Options** aus.
2. Wählen Sie **IP based matching for Hostname based policy resources** aus.
3. Klicken Sie auf **Save Changes**.

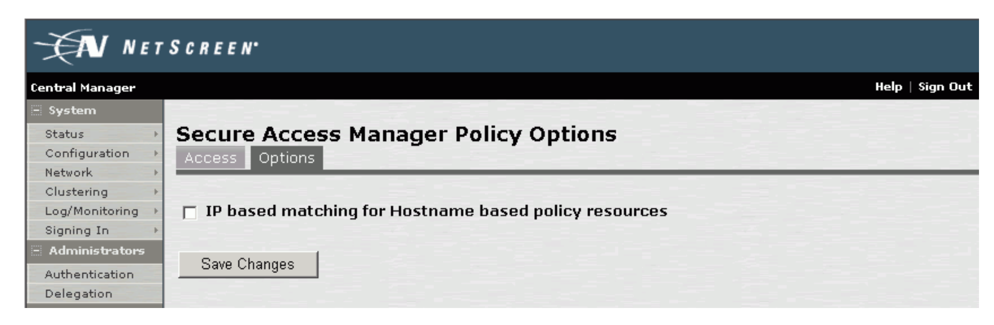


Abbildung 151: **Resource Policies > SAM > Options**

Konfigurieren der Seite „Telnet/SSH“

Die Seite **Resource Policies > Telnet/SSH** enthält die folgenden Registerkarten:

Auf der Seite **Resource Policies > Telnet/SSH** können Sie Folgendes durchführen:

Mithilfe der Aktualisierungsoption sicherer Terminalzugriff können Benutzer eine unverschlüsselte Verbindung mit internen Serverhosts über Telnet-Protokolle herstellen oder in einer verschlüsselten SSH-Sitzung (Secure Shell) über eine webbasierte Terminalsitzungs-Emulation kommunizieren. Diese Funktion unterstützt die folgenden Anwendungen und Protokolle:

- Netzwerkprotokolle
  - Telnet
  - SSH
- Terminaleinstellungen
  - VT100, VT320 und Ableitungen
  - Bildschirmpuffer
- Sicherheit
  - Web-/Clientsicherheit über SSL
  - Hostsicherheit: SSH (sofern erwünscht)

Schreiben einer Telnet/SSH-Ressourcenrichtlinie

Wenn Sie die Zugriffsfunktion Telnet/SSH für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die die Remoteserver angeben, auf die die Benutzer zugreifen dürfen. Wenn das IVE für eine Benutzeranforderung für eine Ressource, die in einer Telnet/SSH-Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Telnet/SSH-Ressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Telnet/SSH-Richtlinie müssen Sie Remoteserver angeben, mit denen Benutzer eine Verbindung herstellen können.
- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.
- **Aktionen:** Eine Telnet/SSH-Ressourcenrichtlinie erlaubt oder verweigert den Zugriff auf einen Server.

Registerkarte „Access“

Über die Registerkarte **Access** können Sie eine Telnet/SSH-Ressourcenrichtlinie schreiben, die angibt, auf welche Anwendungsressourcen Benutzer zugreifen können.

☑ Schreiben einer Telnet/SSH-Ressourcenrichtlinie

So schreiben Sie eine Telnet/SSH-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole **Resource Policies > Telnet/SSH > Access** aus.
2. Klicken Sie auf der Seite **Telnet/SSH Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Server an, für die diese Richtlinie gelten soll.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

- **Policy applies to all roles OTHER THAN those selected below**

  Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Server, die in der Liste **Resources** aufgeführt sind.

   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Server, die in der Liste **Resources** aufgeführt sind.

   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Telnet/SSH Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

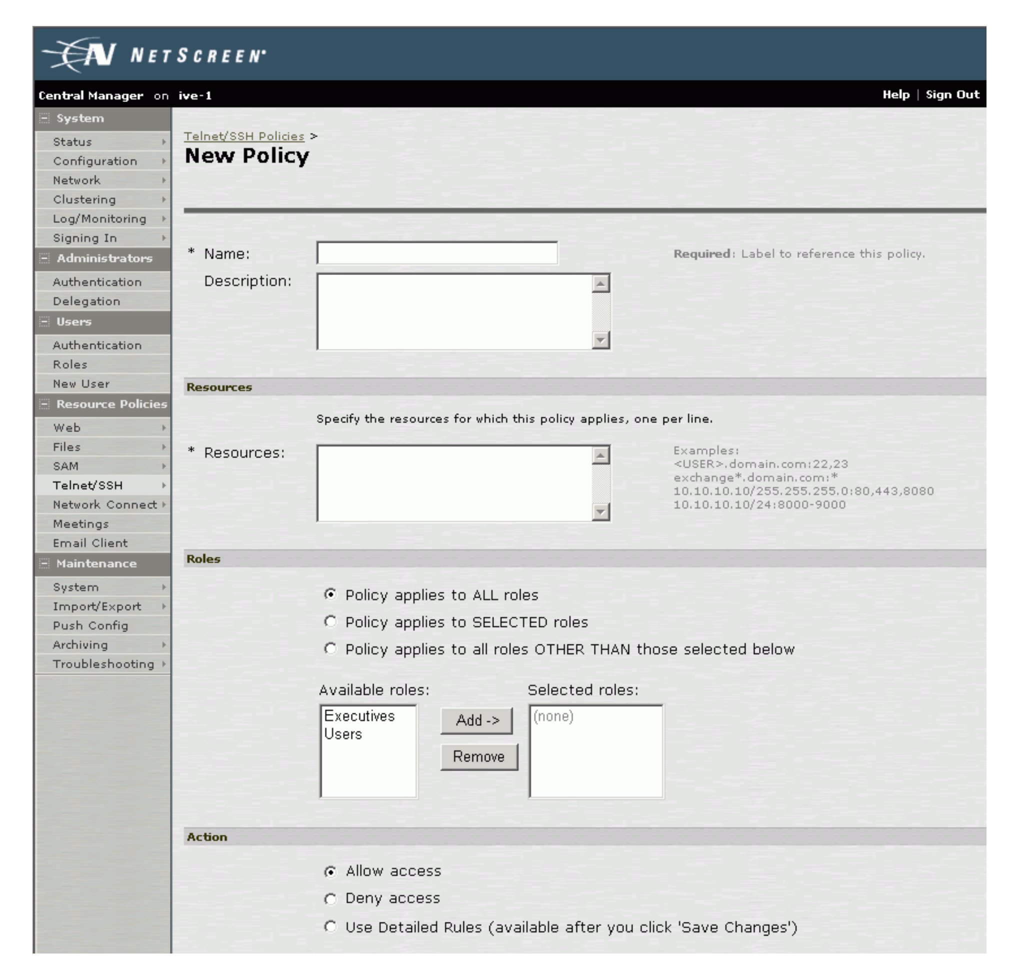


Abbildung 152: **Resource Policies > Telnet/SSH > Access > New Policy**

Registerkarte „Options“

Über die Registerkarte **Options** können Sie die Telnet/SSH-Ressourcenoption so festlegen, dass IP-Adressen mit Hostnamen abgeglichen werden, die in Ihren Telnet/SSH-Ressourcenrichtlinien als Ressourcen angegeben sind. Wenn Sie diese Option aktivieren, sucht das IVE nach IP-Adressen, die einzelnen in einer Telnet/SSH-Ressourcenrichtlinie angegebenen Hostnamen entsprechen. Wenn ein Benutzer versucht, auf einen Server zuzugreifen, indem er eine IP-Adresse anstelle eines Hostnamens angibt, vergleicht das IVE die IP mit den IP-Adressen seiner zwischengespeicherten Liste, um zu bestimmen, ob ein Hostname mit einer IP übereinstimmt. Wenn eine Übereinstimmung vorliegt, akzeptiert das IVE diese als eine Richtlinienübereinstimmung und führt die für die Ressourcenrichtlinie angegebene Aktion durch.

Wenn Sie diese Option aktivieren, stellt das IVE eine Liste mit Hostnamen zusammen, die in den Ressourcenfeldern der einzelnen Telnet/SSH-Ressourcenrichtlinien angegeben sind. Daraufhin wendet das IVE die Option auf diese umfassende Liste mit Hostnamen an.

Hinweis: Diese Option wird nicht auf Hostnamen angewendet, die Platzhalter und Parameter enthalten.

☑ Angeben der Telnet/SSH-Ressourcenoption

So geben Sie die Telnet/SSH-Ressourcenoption an:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Telnet/SSH > Options** aus.
2. Wählen Sie **IP based matching for Hostname based policy resources** aus.
3. Klicken Sie auf **Save Changes**.

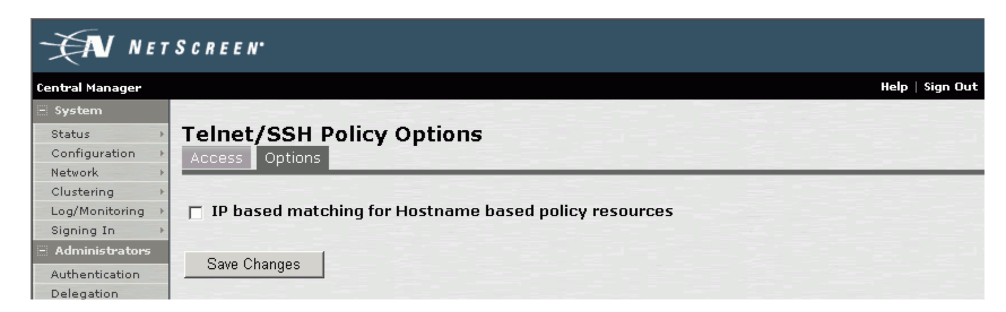


Abbildung 153: **Resource Policies > Telnet/SSH > Options**

Konfigurieren der Seite „Network Connect“

Über die Aktualisierungsoption Network Connect verfügen Sie auf Netzwerkebene über einen sicheren, SSL-basierten Remotezugriff auf ***alle*** Unternehmens-Anwendungsressourcen über das IVE.

Wichtig: Benutzer müssen auf ihrem Windows PC über Administrator- oder Hauptbenutzerberechtigungen verfügen, um das IVE für die Installation des Network Connect-Agent zu aktivieren.

Die Seite **Resource Policies > Network Connect** enthält die folgenden Registerkarten:

Auf der Seite **Resource Policies > Network Connect** können Sie Folgendes durchführen:

Konfigurieren von Network Connect

Wenn Sie die Zugriffsfunktion Network Connect für eine Rolle konfigurieren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Ressourcen ein Benutzer zugreifen darf und von welchen IP-Pools das IVE dem Network Connect-Client-Agent und dem Serverprozess IP-Adressen zuweisen kann. Außerdem müssen Sie den Router so konfigurieren, dass dieser auf die IP-Adresse des internen Ports des IVE als Gateway für Routen von Antworten auf Clientanforderungen über das Netzwerk weist.

Anforderungen für Cluster

Wenn Sie einen Multisite-Cluster ausführen und für jeden Knoten unterschiedliche Netzwerkadressen verwendet werden, müssen Sie folgende Schritte ausführen:

- Konfigurieren Sie eine Richtlinie für IP-Adresspools für die unterschiedlichen Netzwerkadressen, die von den einzelnen Knoten im Cluster verwendet werden.
- Geben Sie für jeden Knoten im Cluster einen IP-Filter an, der nur die für den Knoten verfügbaren Netzwerkadressen herausfiltert.
- Erstellen Sie für den Router einen Zeiger für die IP-Adresse des internen Ports jedes Clusterknotens. Alle vom Router angegebenen IP-Adressen müssen sich im gleichen Subnetzwerk befinden wie der jeweilige Clusterknoten.

Registerkarte „Access“

Über die Registerkarte **Access** können Sie eine Network Connect-Ressourcenrichtlinie schreiben, die angibt, mit welchen Ressourcen Benutzer über Network Connect eine Verbindung herstellen dürfen.

☑ **Schreiben einer Ressourcenrichtlinie für Network Connect-Zugriff:**

So schreiben Sie eine Ressourcenrichtlinie für Network Connect-Zugriff:

1. Wählen Sie in der Webkonsole **Resource Policies > Network Connect > Access** aus.
2. Klicken Sie auf der Seite **Network Connect Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Serverressourcen“ auf Seite 50.

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit definieren Sie Regeln für Ressourcenrichtlinien, die die angegebenen Ressourcen zusätzlich einschränken. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Network Connect Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

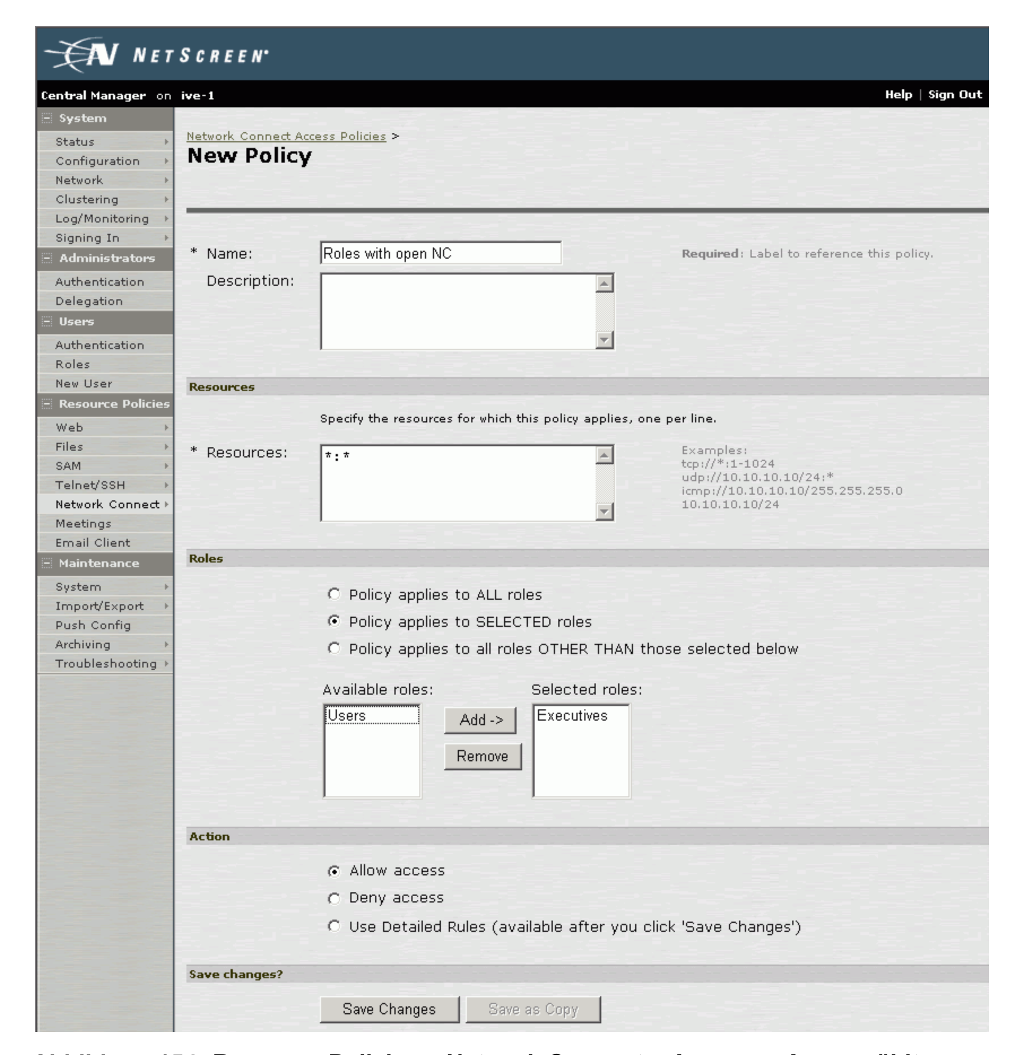


Abbildung 154: Resource Policies > Network Connect > Access > *Ausgewählte Richtlinie* > New Policy

Registerkarte „IP Address Pools“

Über die Registerkarte **IP Address Pools** können Sie eine Network Connect-Ressourcenrichtlinie schreiben, die einen IP-Pool angibt, aus dem das IVE den Server- und Clientprozessen für eine Network Connect-Sitzung eine IP-Adresse zuweist. Wenn ein IVE eine Clientanforderung zum Starten einer Network Connect-Sitzung empfängt, weist es sowohl dem clientseitigen Network Connect-Agent als auch dem serverseitigen IVE-Prozess eine IP-Adresse zu. Das IVE weist diese IP-Adressen anhand der Richtlinien für den IP-Adresspool zu, die auf eine Benutzerrolle zutreffen.

Knoten in einem Cluster mit mehreren Sites nutzen die Konfigurationsinformationen gemeinsam, d. h., dass IVEs in verschiedenen Netzwerken einen IP-Pool gemeinsam nutzen. Da jeder IVE -Knoten die Clientanforderung zum Starten der Network Connect-Sitzung empfangen kann, müssen Sie für den Knoten einen IP-Filter festlegen, der lediglich die für den betreffenden Knoten verfügbaren Netzwerkadressen herausfiltert. Wenn der Clusterknoten eine Anforderung zum Erstellen einer Network Connect-Sitzung empfängt, weist er die zwei IP-Adressen aus dem gefilterten IP-Pool für die Sitzung zu.

☑ Schreiben einer Network Connect-Ressourcenrichtlinie für IP-Adresspools

So schreiben Sie eine Network Connect-Ressourcenrichtlinie für IP-Adresspools:

1. Wählen Sie in der Webkonsole **Resource Policies > Network Connect > IP Address Pools** aus.
2. Klicken Sie auf der Seite **Network Connect IP Address Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Dies ist optional.)
4. Geben Sie unter **Resources** IP-Adressen oder einen IP-Adress-Bereich an, die das IVE Clients zuweisen soll, die den Network Connect-Dienst ausführen. Informationen zum Angeben eines IP-Bereichs finden Sie unter „Angeben von IP-Adresspools“ auf Seite 51.

Da das IVE pro Network Connect-Sitzung zwei IP-Adressen reserviert, müssen Sie eine gerade Anzahl von IP-Adressen angeben. Um z. B. eine Network Connect-Sitzung in einem IVE zuzulassen, geben Sie zwei IP-Adressen an. Um 100 Sitzungen zuzulassen, geben Sie 200 IP-Adressen an.

Hinweis: Wenn in einem LAN oder WAN einen Multi-Unit-Cluster ausführen, muss der IP-Pool Adressen enthalten, die für jeden Knoten im Cluster gültig sind. Konfigurieren Sie dann einen IP-Filter für jeden Knoten, der auf diesen IP-Pool angewendet werden soll.

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Klicken Sie auf **Save Changes**.
7. Ordnen Sie die Richtlinien auf der Seite **Network Connect IP Address Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Registerkarte „Split Tunneling Networks“

Mit der Registerkarte **Split Tunneling Networks** können Sie eine Network Connect-Ressourcenrichtlinie schreiben, die die internen Netzwerke angibt, für die das IVE den Datenverkehr regelt.

☑ Schreiben einer Network Connect-Ressourcenrichtlinie für Netzwerke mit geteilten Tunneln

So schreiben Sie eine Network Connect-Ressourcenrichtlinie für Netzwerke mit geteilten Tunneln:

1. Wählen Sie in der Webkonsole die Optionen **Resource Policies > Network Connect > Split Tunneling Networks** aus.
2. Klicken Sie auf der Seite **Network Connect Split Tunneling Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie (optional).
4. Geben Sie im Bereich **Resources** eine Kombination aus IP-Adresse und Netzmaske für jedes Netzwerk an, für das das IVE den Datenverkehr regelt. Sie können diese Netzwerke auch in der Schreibweise mit '/' (Schrägstrich) angeben.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Klicken Sie auf **Save Changes**.
7. Ordnen Sie die Richtlinien auf der Seite **Network Connect Split Tunneling Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

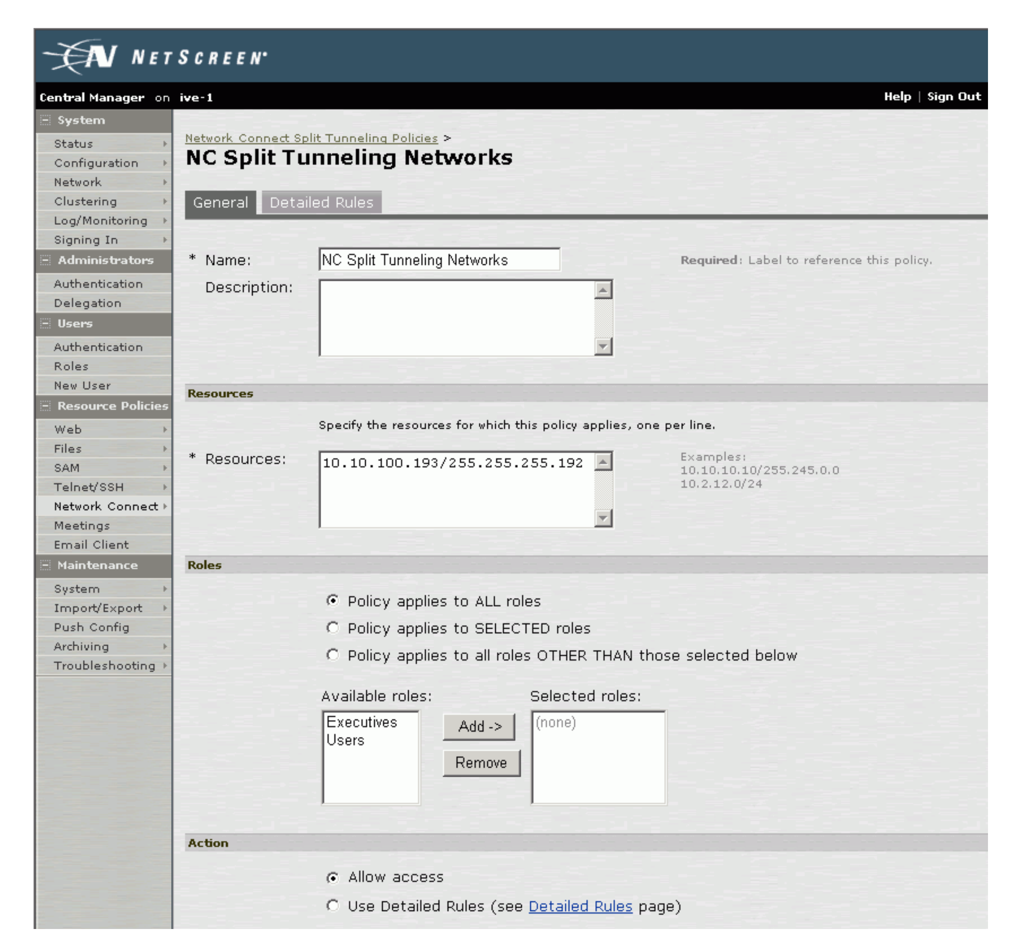


Abbildung 155: Resource Policies > Network Connect > Split Tunneling > NewPolicy

Konfigurieren der Seite „Meetings“

Auf der Seite **Resource Policies > Meetings** können Sie Folgendes durchführen:

Mithilfe der Aktualisierungsoption Secure Meeting können Benutzer innerhalb des gesamten Unternehmens Onlinekonferenzen über eine intuitiv bedienbare Webseite planen und abhalten. Weitere Informationen finden Sie unter „Secure Meeting – Übersicht“ auf Seite 15.

Schreiben einer Ressourcenrichtlinie für Secure Meeting

Im Gegensatz zu anderen Zugriffsfunktionen verfügt Secure Meeting nur über eine Ressourcenrichtlinie, die für *alle* Rollen gilt, für die diese Funktion aktiviert ist. Wenn Sie die Secure Meeting-Zugriffsfunktion für eine Rolle aktivieren, müssen Sie eine Ressourcenrichtlinie erstellen, die angibt, ob das IVE folgende Einstellungen aktivieren soll:

- Sommerzeitanpassung für geplante Konferenzen
- 32-Bit-Farbvorführungen bei Konferenzen
- Automatische E-Mail-Benachrichtigung für Secure Meeting-Gäste

Wenn Sie automatische E-Mail-Benachrichtigungen für Gäste aktivieren, müssen Sie für das Routing von Konferenz-E-Mails einen SMTP-Server verwenden, auf den das IVE zugreifen kann.

Wichtig:

Beim Aktivieren eines SMTP-Servers für Secure Meeting sollten Sie außerdem einen virtuellen Hostnamen für Ihre IVE-Anwendung im Feld **Hostname** der Registerkarte **System > Network > Overview** definieren. Secure Meeting verwendet den angegebenen Hostnamen zum Einfügen der Konferenz-URLs in Benachrichtigungs-E-Mails und für SMTP-Aufrufe. Wenn dem IVE verschiedene Namen zugeordnet sind und Sie keinen virtuellen Hostnamen angeben, müssen Sie vor dem Erstellen einer Konferenz u. U. einschränken, unter welchem Namen sich IVE-Benutzer anmelden können. Beispiel: Wenn das IVE einem internen Namen zugeordnet ist (wie **vertrieb.acmegizmo.com**), der nur innerhalb der Firmenfirewall gültig ist, sowie einem weiteren Namen (wie **partner.acmegizmo.com**), der überall verwendet werden kann, sollten sich IVE-Benutzer vor dem Erstellen einer Konferenz unter **partner.acmegizmo.com** anmelden. Andernfalls erhalten Gäste ohne IVE E-Mal-Benachrichtigungen, in denen Verknüpfungen mit einem nicht erreichbaren IVE enthalten sind.

☑ Schreiben einer Ressourcenrichtlinie für E-Mail-Benachrichtigungen von Secure Meeting

So schreiben Sie eine Secure Meeting-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole **Resource Policies > Meetings** aus.
2. Geben Sie in der Liste **Observe DST in this default timezone** die Zeitzone an, in der sich das IVE befindet. In diesem Fall erben alle Konferenzen standardmäßig die Sommerzeitanpassung für die angegebene Zone. Sie können auch **Do not observe DST** auswählen, um zu verhindern, dass das IVE die Sommerzeitanpassungen vornimmt.

   Hinweis: Die Benutzer können über die Seite **Preferences** Ihre Sommerzeitanpassungen einzeln außer Kraft setzen. In diesem Fall sind sie von Änderungen, die Sie auf der Seite **Meetings Policies** vornehmen, nicht betroffen.

3. Wählen Sie **Enable 32-bit (True Color) Presentations** aus, um Benutzern True Color-Präsentationen zu ermöglichen. Standardmäßig stellt Secure Meeting den Benutzern Anwendungen bereit, die dieselbe Farbtiefe verwenden wie der Desktop des Vorführenden (bis zu 32-Bit-Farbe). Wenn Sie diese Option nicht auswählen und ein Benutzer eine Anwendung mit 32-Bit-Farbe vorführt, ändert Secure Meeting das Bild jedoch zu 16-Bit-Farbe, um die Leistung zu verbessern.
4. Wählen Sie im Bereich **Email meeting notifications** die Option **Enabled**, um den SMTP-E-Mail-Server zu aktivieren. Gehen Sie anschließend folgendermaßen vor:
   - Geben Sie im Feld **SMTP Server** die IP-Adresse oder den Hostnamen eines SMTP-Servers ein, der E-Mail-Nachrichten von der Appliance an die Konferenzgäste weiterleiten kann.
   - Geben Sie bei entsprechender Anforderung vom SMTP-Server in den Feldern **SMTP Login** und **SMTP Password** einen gültigen Anmeldenamen und ein Kennwort für den angegebenen E-Mail-SMTP-Server ein.
   - Geben Sie im Feld **SMTP Email** Ihre E-Mail-Adresse oder die Adresse eines anderen Administrators ein. Secure Meeting verwendet die angegebene Adresse als E-Mail-Adresse des Absenders, wenn der Ersteller der E-Mail-Nachricht im IVE keine eigene E-Mail-Adresse konfiguriert hat.
5. Klicken Sie auf **Save Changes**.
6. Konfigurieren Sie Secure Meeting-Einstellungen für einzelne Rollen anhand der Anweisungen in „Registerkarte „Meetings““ auf Seite 433.

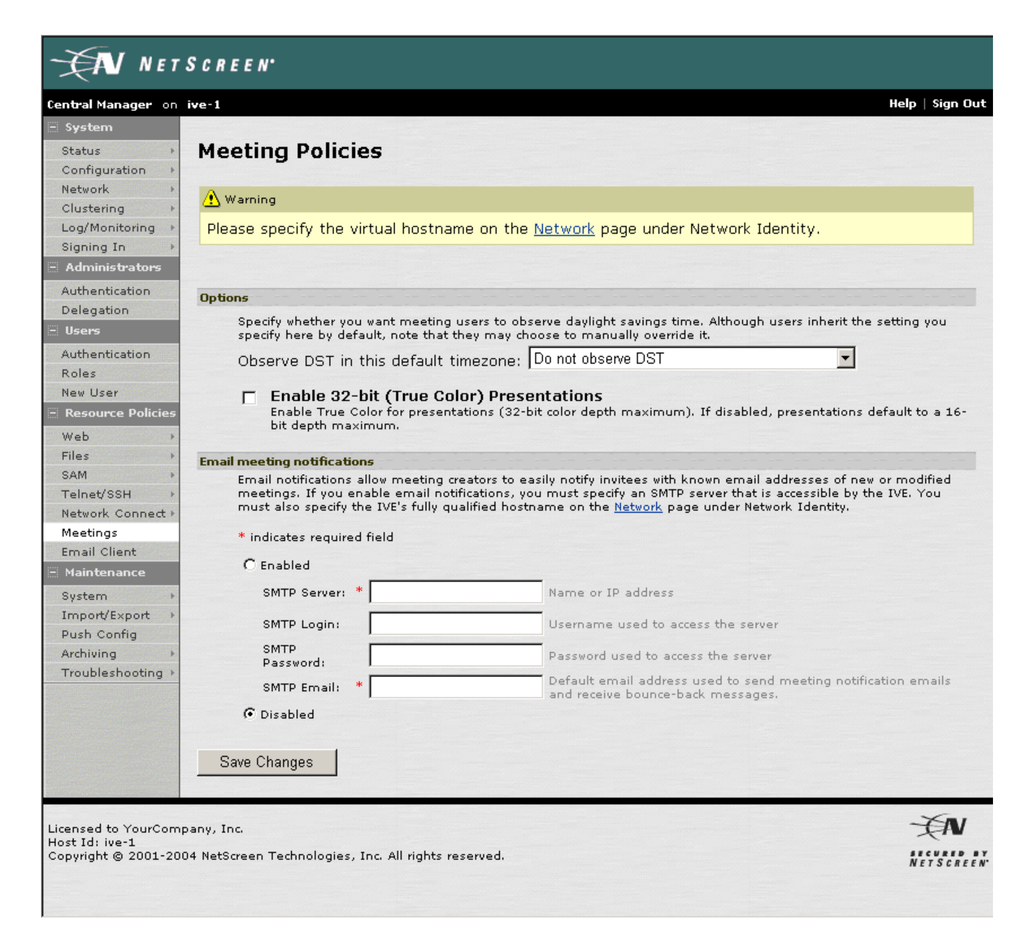


Abbildung 156: **Resource Policies > Meetings**

Konfigurieren der Seite „Email Client“

Auf der Seite **Resource Policies > E-Mail-Client** können Sie Folgendes durchführen:

Durch die Aktualisierungsoption Secure Email Client können Remotebenutzer über einen Webbrowsers und eine Internetverbindung auf standardbasierte E-Mail-Anwendungen wie Outlook Express, Netscape Communicator oder Eudora von Qualcomm zugreifen. Weitere Informationen finden Sie unter „E-Mail-Client – Übersicht“ auf Seite 89.

Schreiben einer Ressourcenrichtlinie für E-Mail-Client

Wenn Sie die Zugriffsfunktion E-Mail-Client für eine Rolle aktivieren, müssen Sie eine Ressourcenrichtlinie erstellen, die Einstellungen für den Mailserver angibt. Im Gegensatz zu anderen Zugriffsfunktionen verfügt Secure Email Client nur über eine Ressourcenrichtlinie, die für *alle* Rollen gilt, für die diese Funktion aktiviert ist. Wenn Sie den E-Mail-Client-Dienst für Benutzer aktivieren, müssen Sie IMAP-, POP- und SMTP-Mailserverinformationen und Einstellungen für die Benutzerauthentifizierung angeben. Das IVE fungiert als E-Mail-Proxy für den bzw. die angegebenen Server.

Das IVE unterstützt mehrere Mailserver. Sie können festlegen, dass alle Benutzer einen Standardmailserver verwenden müssen, oder Sie können Benutzern die Möglichkeit geben, einen benutzerdefinierten SMTP- und IMAP- bzw. POP-Mailserver anzugeben. Wenn Sie Benutzern das Festlegen eines benutzerdefinierten Mailservers ermöglichen, müssen diese die Servereinstellungen über das IVE vornehmen. Der IVE-Server verwaltet die E-Mail-Benutzernamen, um Namenskonflikte zu vermeiden.

☑ Schreiben einer E-Mail-Client-Ressourcenrichtlinie für Mailserver

So schreiben Sie eine E-Mail-Client-Ressourcenrichtlinien für Mailserver:

1. Wählen Sie in der Webkonsole **Resource Policies > E-Mail-Client** aus.
2. Klicken Sie unter **Email Client Support** auf **Enabled**.

3. Wählen Sie unter **Email Authentication Mode** eine der folgenden Optionen aus:
   - **Web-based email session**

     Benutzer müssen eine einmalige E-Mail-Einrichtung für das IVE vornehmen. Anschließend konfigurieren sie ihren E-Mail-Client so, dass der Benutzername und das Kennwort verwendet werden, die durch die E-Mail-Einrichtung für das IVE generiert werden. Es empfiehlt sich, dass die Benutzer sich an dem IVE anmelden, um eine E-Mail-Sitzung zu starten. (Standardeinstellung)
   - **Combined IVE and mail server authentication**

     Benutzer konfigurieren ihren E-Mail-Client so, dass die folgenden Anmeldeinformationen verwendet werden:
     - Benutzername: Der normale Benutzername eines Benutzers für den Mailserver oder ein Benutzername, der beim E-Mail-Setup für das IVE generiert wird, wenn eine der folgenden Bedingungen zutrifft:
       – der Benutzer verfügt über mehrere Benutzernamen für den Mailserver
       – die Benutzernamen auf dem IVE-Server und dem Mailserver sind unterschiedlich
     - Kennwort: Das IVE-Kennwort des Benutzers, auf das ein benutzerdefinierbares Trennzeichen für Anmeldeinformationen und das Mailserverkennwort des Benutzers folgen.

     Benutzer müssen sich nicht am IVE anmelden, um E-Mail zu verwenden.
   - **Mail server authentication only**

     Benutzer konfigurieren ihren E-Mail-Client so, dass ihre normalen Mailserver-Benutzernamen und -Kennwörter verwendet werden. Benutzer müssen sich nicht am IVE anmelden, um E-Mail zu verwenden oder zu konfigurieren.

     Hinweis: Die Benutzer können ihre Benutzernamen und Kennwörter für E-Mail problemlos auf der Seite **Email Setup** ermitteln.

4. Geben Sie unter **Default Server Information** Ihre Mailserverdaten an. Das IVE fungiert als E-Mail-Proxy für diesen Server.

   Wichtig: Sie können nur einen Standardmailserver angeben. Wenn Benutzer E-Mail-Nachrichten von mehreren SMTP- und POP- bzw. IMAP-Servern abrufen müssen, bieten Sie Ihnen durch Aktivieren des entsprechenden Kontrollkästchens die Möglichkeit, weitere Mailserver zu definieren. Wenn Sie Benutzern die Festlegung benutzerdefinierter Server ermöglichen, müssen die Benutzer diese Informationen auf ihrer IVE-Seite „Email Setup“ eingeben.

5. Geben Sie unter **Email Session Information** Folgendes an:
   - Einen **Idle Timeout**-Wert, der angibt, wie lange sich die E-Mail-Sitzung eines Benutzers im Leerlauf befinden kann, bevor das IVE die E-Mail-Sitzung beendet.
   - Einen Wert für **Max. Session Length**, der angibt, wie lange sich die E-Mail-Sitzung eines Benutzers im Leerlauf befinden kann, bevor das IVE die E-Mail-Sitzung beendet.
6. Klicken Sie auf **Save Changes**.

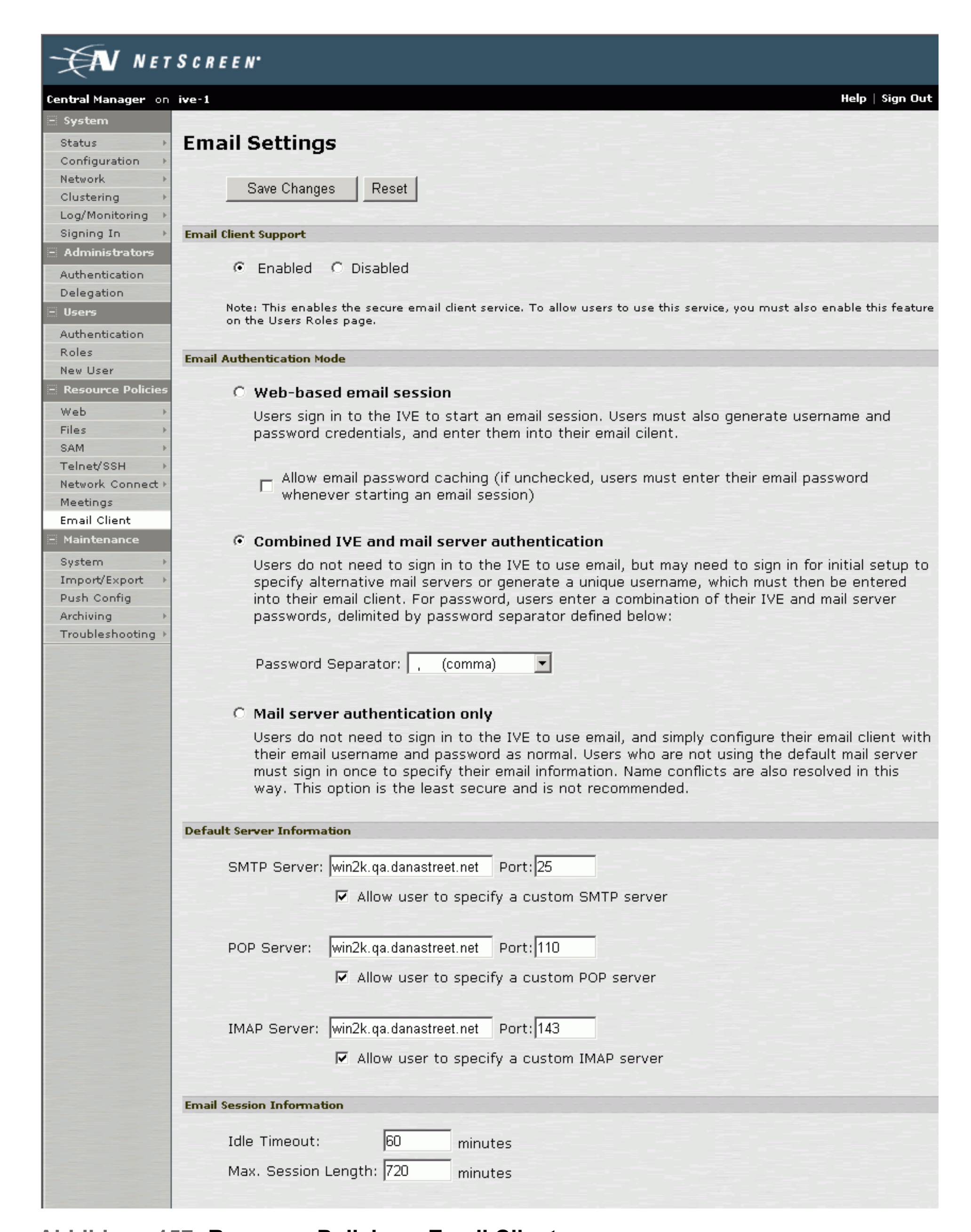


Abbildung 157: **Resource Policies > Email Client**

Konfigurieren der Seite „System“

Die Seite **Maintenance > System** enthält die folgenden Registerkarten:

Auf der Seite **Maintenance > System** können Sie Folgendes durchführen:

Registerkarte „Platform“

☑ Neustarten, Herunterfahren und Testen der Verbindung

Auf der Seite **Platform** können Sie die IVE-Verbindung neu starten, neu hochfahren, herunterfahren oder testen sowie Systemdaten anzeigen (beispielsweise den IVE-Hostnamen und die Zeit des letzten Neustarts). Informationen zur Handhabung der folgenden Situationen finden Sie in „Anhang A: “ auf Seite 567 :

- Sie haben Ihre Anmeldedaten vergessen.
- Sie haben die IP-Beschränkungen so eingestellt, dass Sie sich nicht mehr am Gerät anmelden können.
- Sie möchten das System in den vorherigen Zustand zurücksetzen.
- Sie müssen das System auf die Werkseinstellungen zurücksetzen.

So starten Sie die Serververbindung neu, fahren sie neu hoch bzw. herunter oder testen diese:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > System > Platform** aus.
2. Wählen Sie eine der folgenden Optionen aus:
   - **Restart IVE** – Startet das IVE neu.
   - **Reboot IVE** – Fährt das IVE neu hoch.

- **Shut down IVE** – Fährt das IVE herunter, wobei Sie den Reset-Schalter an der Appliance drücken müssen, um den Server neu zu starten. Beachten Sie, dass das Gerät nach dem Herunterfahren des Servers eingeschaltet bleibt.
- **Test Server Connectivity** – Sendet einen ICMP-Ping-Befehl vom IVE an alle Server, die vom IVE gemäß der Konfiguration verwendet werden, und testet ihre Verbindung. Der Status der einzelnen Server wird unter **Server Connectivity Results** aufgeführt.

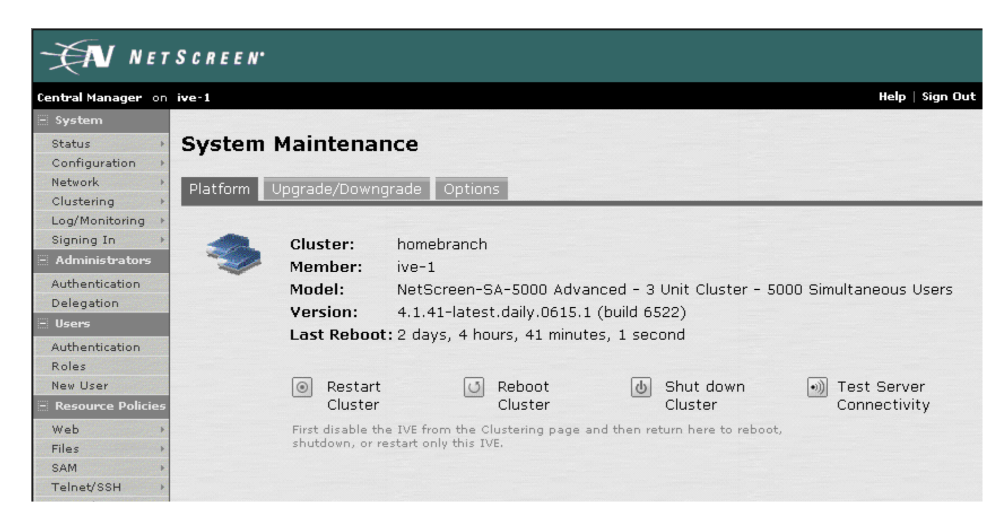


Abbildung 158: **Maintenance > System > Platform**

Registerkarte „Upgrade/Downgrade“

Sie installieren ein anderes Dienstpaket, indem Sie zuerst von der Juniper Networks-Supportsite die Software herunterladen und diese dann über die Webkonsole hochladen. Paketdateien werden verschlüsselt und signiert, sodass der IVE-Server nur gültige, von Juniper Networks ausgegebene Pakete akzeptiert. Mit dieser Maßnahme wird verhindert, dass der IVE-Server als „Trojanische Pferde“ bezeichnete Programme akzeptiert.

Dieses Feature wird meist dazu verwendet, Aktualisierungen auf neuere Versionen der Systemsoftware durchzuführen. Sie können jedoch mit diesem Verfahren die Systemsoftware auch auf eine ältere Version herunterstufen oder alle aktuellen Konfigurationseinstellungen löschen und eine neue Ausgangsbasis schaffen. Ein Rollback zu einem vorherigen Systemzustand ist auch über die serielle Konsole möglich. Dieser Vorgang ist unter „Rollback zu einem vorherigen Systemzustand“ auf Seite 568 beschrieben.

Hinweis: Die Installation eines neuen Dienstpakets kann einige Minuten dauern. Das IVE muss anschließend neu gestartet werden. Da bei diesem Vorgang die vorhandenen Systemdaten gesichert werden, lässt sich die Installationsdauer verkürzen, indem der Inhalt des Systemprotokolls vor der Installation eines Dienstpakets gelöscht wird.

☑ Installieren eines Juniper Networks-Softwaredienstpakets

Exportieren Sie vor der Installation eines neuen Dienstpakets die aktuelle Systemkonfiguration, die lokalen Benutzerkonten, die Lesezeichen der Benutzer und die Rollen- und Richtlinieninformationen, wie unter „Konfigurieren der Seite „Import/Export““ auf Seite 530 erläutert.

So installieren Sie ein Dienstpaket:

1. Navigieren Sie zur Juniper Networks-Supportsite, und rufen Sie das gewünschte Dienstpaket ab.
2. Wählen Sie in der Webkonsole die Option **Maintenance > System > Upgrade/Downgrade**. aus.
3. Klicken Sie auf **Browse**, um das von der Supportsite heruntergeladene Dienstpaket auf der Festplatte zu suchen. Wenn Sie die aktuellen Konfigurationseinstellungen löschen, aber weiterhin dieselbe IVE-Version verwenden möchten, wählen Sie das derzeit in Ihrer Appliance installierte Dienstpaket aus.
4. Wenn Sie die Software auf ein älteres Dienstpaket herunterstufen oder die Konfigurationseinstellungen löschen, wählen Sie **Delete all system and user data**.

   Wichtig: Wenn Sie das IVE zurücksetzen und mit dieser Option alle System- und Benutzerdaten aus der Appliance löschen möchten, müssen Sie vor der erneuten Systemkonfiguration die Netzwerkverbindungen wiederherstellen. Beachten Sie außerdem, dass kein Rollback auf eine ältere IVE-Version als 3.1 durchgeführt werden kann.

5. Wählen Sie die Dienstpaketdatei aus, und klicken Sie auf **Install Now**.



Abbildung 159: **Maintenance > System > Upgrade/Downgrade**

Registerkarte „Options“

☑ Aktivieren von Versionsüberwachung und Beschleunigerkarten

Damit das System auf dem neuesten Stand und sicher bleibt, können Sie sich vom IVE automatisch über wichtige Softwarepatches und -aktualisierungen benachrichtigen lassen. Hierzu werden die folgenden Daten an Juniper Networks gemeldet: Name Ihrer Firma, MD5-Hash Ihrer Lizenzeinstellungen und Informationen zur aktuellen Softwareversion. Auf der Seite **Options** können außerdem Beschleunigerkarten zur Leistungssteigerung aktiviert werden.

Hinweis: Die Einstellungen für die Beschleunigerkarte werden nur angezeigt, wenn Sie ein A5000-IVE mit der entsprechenden Karte erworben haben.

So aktivieren Sie automatische Aktualisierungen und Beschleunigerkarten:

1. Wählen Sie in der Webkonsole die Option **Maintenance > System > Options** aus.
2. Aktivieren Sie das Kontrollkästchen **Automatic Version Monitoring**, um automatisch über wichtige Softwarepatches und -aktualisierungen benachrichtigt zu werden.

   Wichtig: Zum Schutz Ihres Systems wird dringend empfohlen, diesen automatischen Dienst zu aktivieren. Falls nötig, können Sie ihn jedoch auch deaktivieren.

3. Aktivieren Sie das Kontrollkästchen **Enable gzip compression**, um die Datenmenge zu verringern, die an Browser mit Unterstützung von HTTP-Komprimierung gesendet wird. Dies kann für einige Benutzer das Herunterladen von Seiten beschleunigen.
4. Aktivieren Sie das Kontrollkästchen **SSL Accelerator**, damit die Ver- und Entschlüsselung von SSL-Handshakes von der Appliance an die Beschleunigerkarte delegiert wird (optional).
5. Aktivieren Sie das Kontrollkästchen **ZIP Accelerator**, damit alle HTML-, JavaScript- und CSS-Daten komprimiert werden, auf die beim Webbrowsing oder bei der Dateinavigation zugegriffen wird (optional).
6. Klicken Sie auf **Save Changes**.

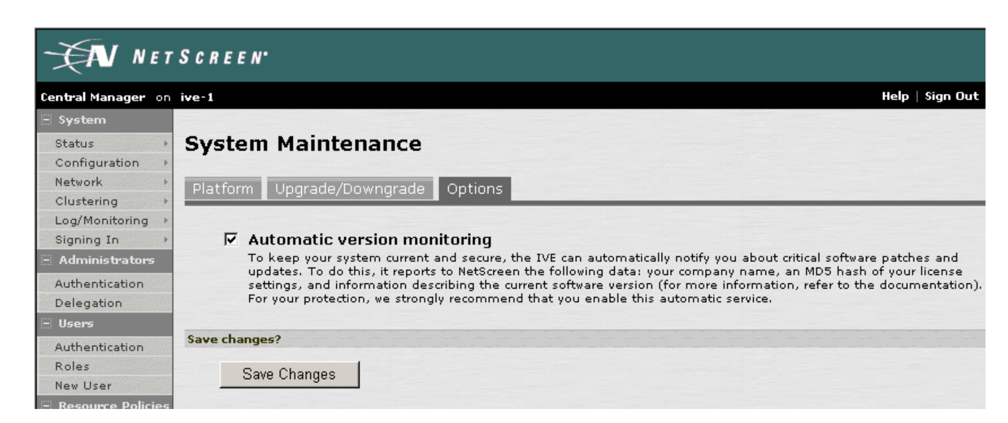


Abbildung 160: **Maintenance > System > Options**

Konfigurieren der Seite „Import/Export“

Die Seite **Maintenance > Import/Export** enthält die folgenden Registerkarten:

Auf der Seite **Maintenance > Import/Export** können Sie Folgendes durchführen:

Registerkarte „Configuration“

Mithilfe dieser Registerkarte können Sie eine Systemkonfigurationsdatei importieren oder exportieren. Die Systemkonfigurationsdatei enthält alle System- und Netzwerkeinstellungen. Weitere Informationen zum Festlegen eines Archivierungsplans für die Serverkonfiguration finden Sie unter „Planen der Archivierung von Systemdaten auf einem externen FTP-Server“ auf Seite 541.

☑ Exportieren einer Systemkonfigurationsdatei

So exportieren Sie eine Systemkonfigurationsdatei:

1. Wählen Sie in der Webkonsole die Optionen **System > Import/ Export > Configuration** aus.
2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.
3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

Wichtig: Beim Exportieren einer Access Series FIPS-Konfigurationsdatei müssen Sie beachten, dass in dieser Datei auch Informationen über die Security World des Geräts enthalten sind. Daher benötigen Sie eine Administratorkarte, die der Security World zugeordnet ist, um die Konfigurationsdatei auf ein anderes Gerät importieren zu können.

☑ Importieren einer Systemkonfigurationsdatei

Beim Importieren einer Systemkonfigurationsdatei können Sie das Serverzertifikat und die IP-Adresse oder die Netzwerkeinstellungen des IVE-Servers aus den importierten Informationen ausschließen. Um beispielsweise mehrere IVEs hinter einem Load-Balancer einzurichten, importieren Sie alle Daten außer der IP-Adresse. Um ein IVE als Sicherungsserver einzurichten, importieren Sie alle Daten außer dem digitalen Zertifikat und den Netzwerkeinstellungen.

Hinweis:

- Beim Importieren einer Konfigurationsdatei mit Lizenzen erhalten im IVE die bestehenden Lizenzen Vorrang, die gegenwärtig auf dem IVE installiert sind. Archivierte Lizenzen werden nur importiert, wenn auf dem IVE gegenwärtig keine Lizenzen vorhanden sind.
- Sie können eine Access Series FIPS-Konfigurationsdatei in einen Nicht-Access Series FIPS-Computer und umgekehrt importieren, sofern Sie nicht das Zertifikat und die Security World importieren.

So importieren Sie eine Konfigurationsdatei:

1. Wählen Sie in der Webkonsole die Optionen **System > Import/ Export > Configuration** aus.
2. Geben Sie an, ob Sie das Serverzertifikat importieren möchten. Das Zertifikat wird nur importiert, wenn Sie das Kontrollkästchen **Import Server Certificate?** aktivieren.

   Wichtig: Beim Importieren eines Serverzertifikats auf ein Access Series FIPS-System müssen Sie ein Zertifikat auswählen, bei dem ein FIPS-kompatibler privater Schlüssel verwendet wird. Um FIPS-Kompatibilität zu gewährleisten, wählen Sie ein Zertifikat und die zugehörigen privaten Security World-Schlüssel aus, die auf einem Access Series FIPS-System erzeugt wurden.

3. Wählen Sie eine Importoption aus. Beachten Sie folgende Punkte:
   - Wenn Sie die IP-Adresse ausschließen, wird die IP-Adresse des Servers beim Importieren der Datei nicht geändert.
   - Wenn Sie die Netzwerkeinstellungen ausschließen, werden die Informationen auf der Seite **System > Network Settings** (Einstellungen für internen Port, externen Port und statische Routen) beim Importieren der Datei nicht geändert.
4. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung `system.cfg` heißt.

5. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.
6. Klicken Sie auf **Import Config**.

Wichtig: Beim Importieren eines Serverzertifikats und der zugehörigen Security World auf ein Access Series FIPS-Gerät müssen Sie die Initialisierung der Security World mit der seriellen Konsole und mit einer Administratorkarte abschließen, die der neuen, importierten Security World zugeordnet ist. Weitere Informationen finden Sie unter „Wiederherstellen einer archivierten Security World (nur Access Series FIPS)“ auf Seite 576.

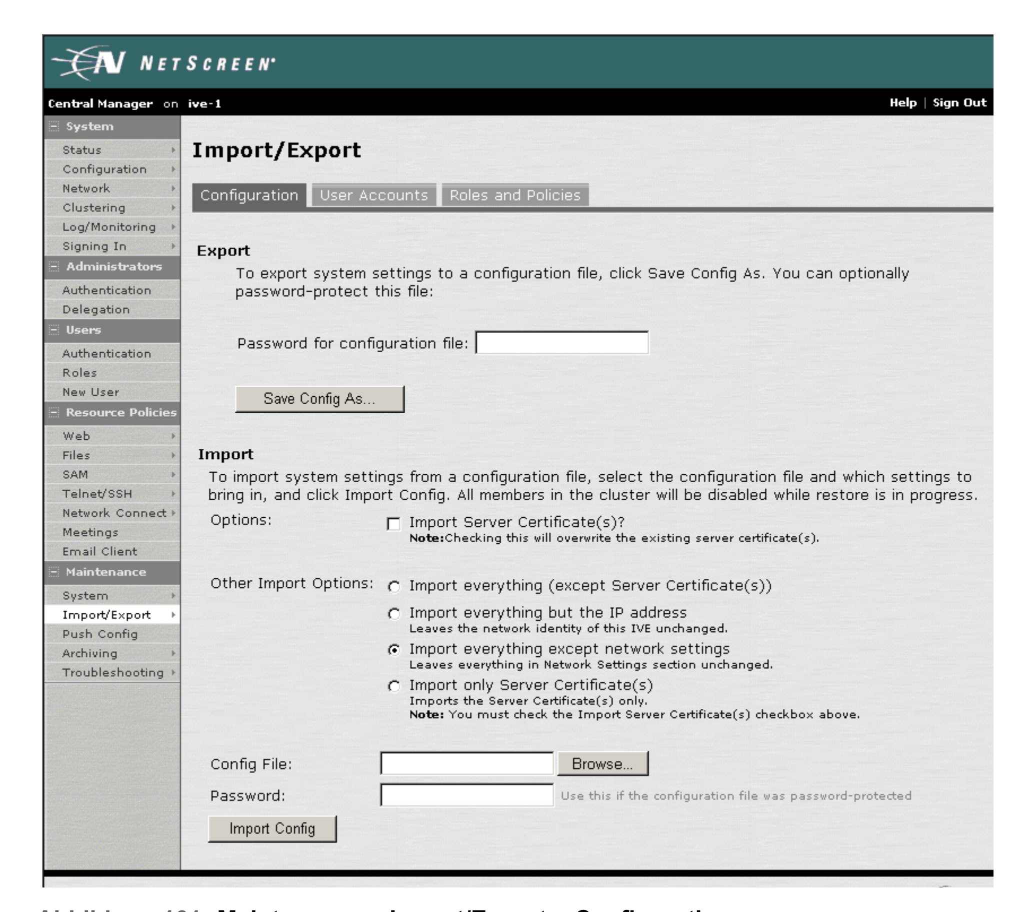


Abbildung 161: **Maintenance > Import/Export > Configuration**

Registerkarte „User Accounts“

Mithilfe dieser Registerkarte können Sie lokale Benutzerkonten importieren oder exportieren. In der Benutzerkontendatei sind sämtliche lokalen Benutzer enthalten, die Sie für alle lokalen Authentifizierungsserver definiert haben. Weitere Informationen zum Festlegen eines Archivierungsplans für Benutzerdatensätze finden Sie unter „Planen der Archivierung von Systemdaten auf einem externen FTP-Server“ auf Seite 541.

☑ Exportieren lokaler Benutzerkonten

So exportieren Sie eine Systemkonfigurationsdatei:

1. Wählen Sie in der Webkonsole die Optionen **System > Import/ Export > Configuration** aus.
2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.
3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

☑ Importieren lokaler Benutzerkonten

So importieren Sie lokale Benutzerkonten:

1. Wählen Sie in der Webkonsole die Optionen **System > Import/ Export > User Accounts** aus.
2. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung `user.cfg` heißt.
3. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.
4. Klicken Sie auf **Import Config**.

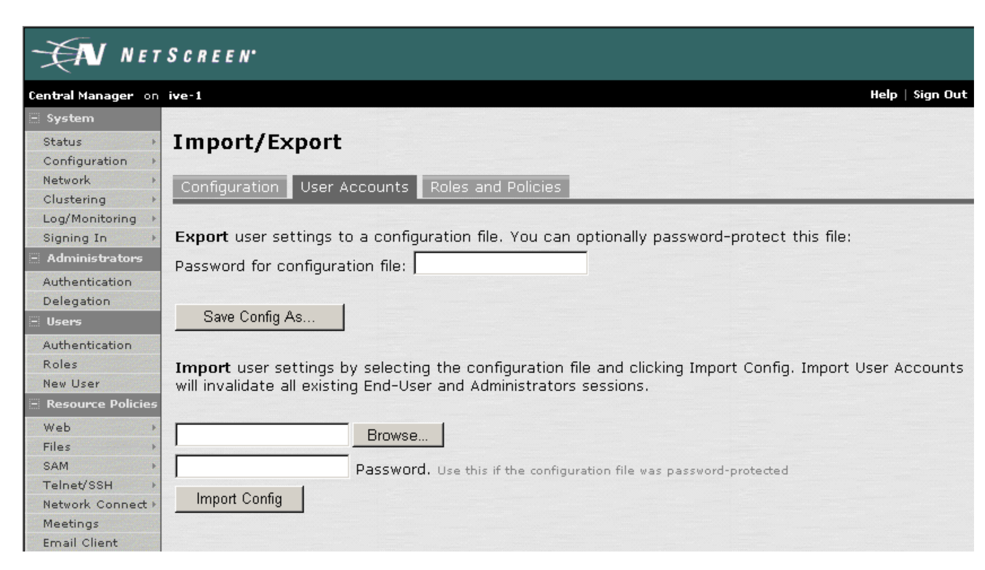


Abbildung 162: **Maintenance > Import/Export > User Accounts**

Registerkarte „Roles and Policies“

Die Seite **Maintenance > Import/Export > Roles and Resources** ermöglicht das Exportieren ausgewählter delegierter Administrationsrollen, Benutzerrollen und Ressourcenrichtlinien auf ein IVE und das anschließende Reimportieren auf ein anderes IVE. (Zum Kopieren von Rollen und Ressourcenrichtlinien aus einem IVE auf ein anderes können Sie auch die Konfigurationsübertragung (Seite 538) verwenden.)

Wichtig: Es wird nicht empfohlen, eine XML-Datei vor dem Importieren auf ein IVE zu verändern. Dies kann Konfigurationsfehler verursachen, die schwer aufzuspüren und zu beheben sind.

☑ Exportieren von Rollen und Ressourcenrichtlinien

So exportieren Sie Rollen und Ressourcenrichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Roles and Policies > Export** aus.
2. Aktivieren Sie das Kontrollkästchen **Delegated Admin Roles**, um delegierte Administrationsrollen zu kopieren. Gehen Sie anschließend folgendermaßen vor:

- Wählen Sie **All roles** aus, um alle delegierten Administrationsrollen zu kopieren.
- Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen kopieren möchten.

3. Aktivieren Sie das Kontrollkästchen **User Roles**, um Benutzerrollen zu kopieren. Gehen Sie anschließend folgendermaßen vor:
   - Wählen Sie **All roles** aus, um alle delegierten Administratorrollen zu kopieren.
   - Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen kopieren möchten.
4. Aktivieren Sie das Kontrollkästchen **Resource Policies**, um Ressourcenrichtlinien zu kopieren. Aktivieren Sie anschließend die Kontrollkästchen für die Typen von Ressourcenrichtlinien, die Sie kopieren möchten, beispielsweise Richtlinien für Zugriffssteuerung, Zwischenspeicherung oder selektives Neuschreiben.
5. Klicken Sie auf **Export Configuration**, um die Informationen in einer XML-Datei zu speichern.

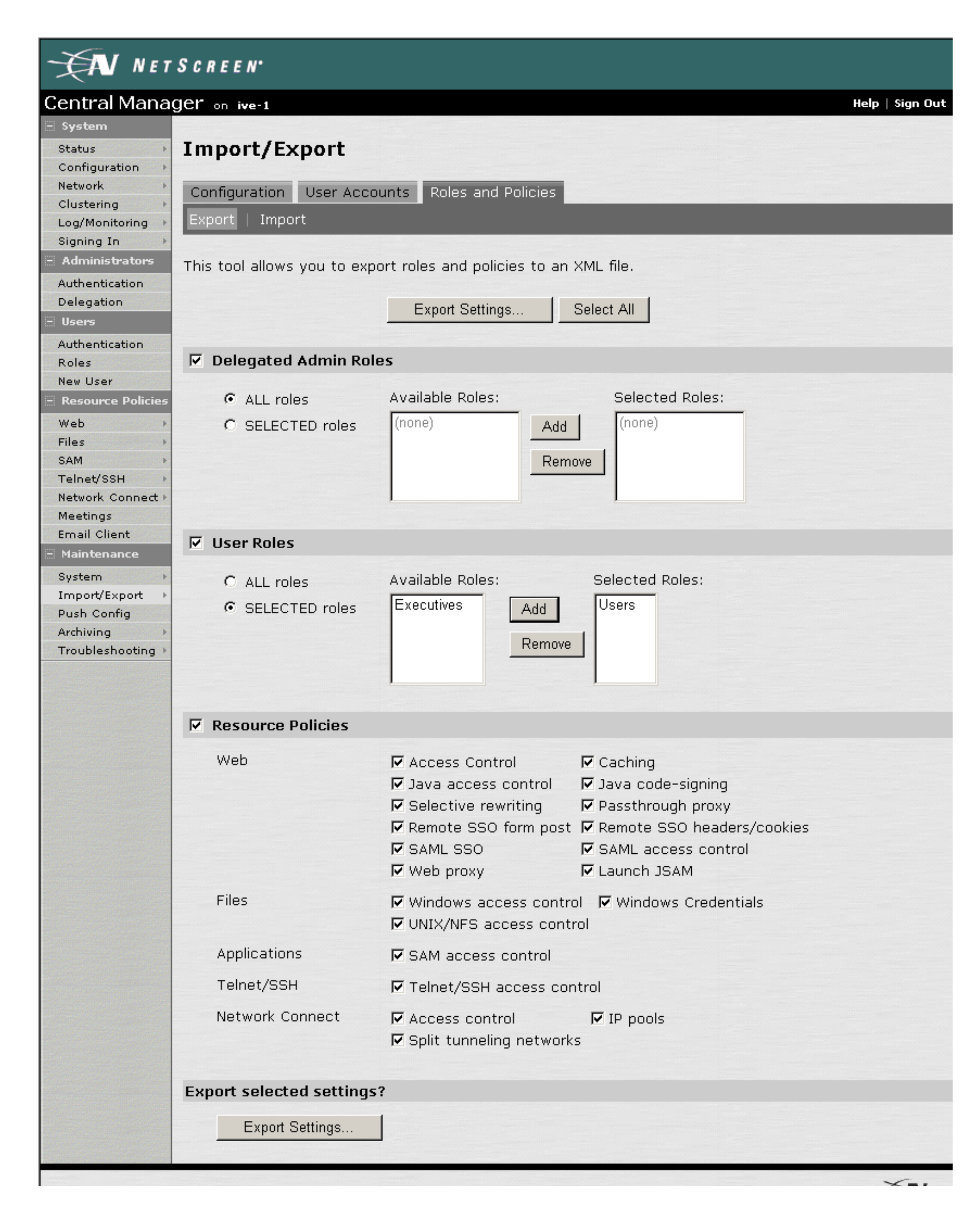


Abbildung 163: Maintenance > Import/Export > Roles and Policies > Export

☑ Importieren von Rollen und Ressourcenrichtlinien

So importieren Sie Rollen und Ressourcenrichtlinien:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Import/Export > Roles and Policies > Import** aus.
2. Navigieren Sie zu dem Verzeichnis mit der XML-Datendatei, die Sie importieren möchten.
3. Aktivieren Sie das Kontrollkästchen **Overwrite duplicate settings**, um die Einstellungen auf dem Ziel-IVE mit Einstellungen zu überschreiben (nicht anzuhängen), die in der XML-Datei enthalten sind (optional).
4. Klicken Sie auf **Import Settings**.

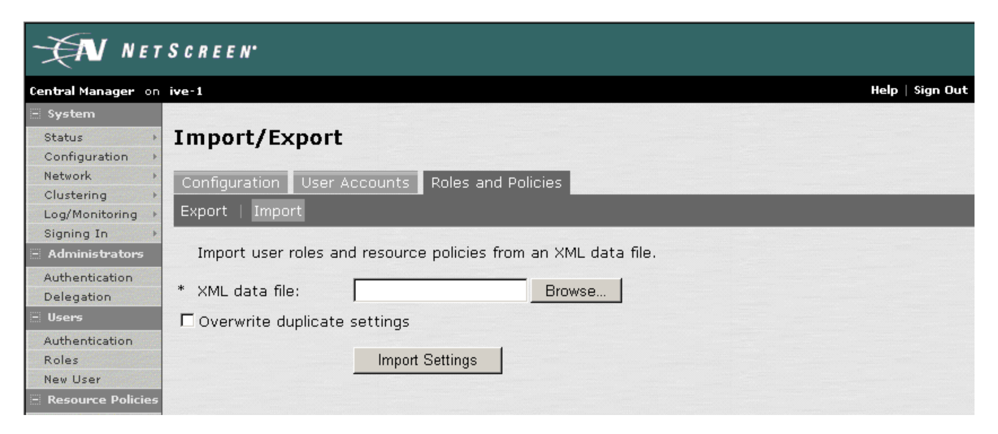


Abbildung 164: **Maintenance > Import/Export > Roles and Policies > Import**

Konfigurieren der Seite „Push Config“

☑ Kopieren von Rollen und Ressourcenrichtlinien zwischen IVEs

Auf der Seite **Maintenance > Push Config** können ausgewählte delegierte Administrationsrollen, Benutzerrollen und Ressourcenrichtlinien über Konfigurationsübertragung von einem IVE auf ein anderes IVE übertragen werden. Diese Funktion ermöglicht eine einfache Konfigurationsverwaltung für ein gesamtes Unternehmen, ohne dass IVE-Appliances in Cluster aufgeteilt werden müssen. Mithilfe der Konfigurationsübertragung können Sie gezielt entscheiden, welche delegierten Administrationsrollen, Benutzerrollen und Typen von Ressourcenrichtlinien unternehmensweit kopiert werden sollen. Beachten Sie, dass die Konfigurationsübertragung nur mit dem Central Manager-Paket verfügbar ist (Seite 67).

Um eine Konfiguration zu übertragen, müssen Sie Administratorkonten auf beiden IVEs erstellen. Die Konfigurationsübertragungs-Funktion meldet sich dann anhand der Administratorinformationen automatisch auf dem Ziel-IVE an. Beachten Sie beim Erstellen eines Administratorkontos Folgendes:

- Sie müssen der **.Administrators**-Rolle zugeordnet sein, d. h. einen „Superadministrator“ mit vollen Administratorberechtigungen erstellen.
- Das Zieladministratorkonto für das IVE muss Authentifizierung mit statischen Kennwörtern oder 2-Faktor-Tokens verwenden, die keine Authentifizierung vom Typ Challenge-Response verwenden. (Zertifikate, Soft ID und Defender-Authentifizierung werden z. B. nicht unterstützt.)
- Sie dürfen das Administratorkonto nicht so konfigurieren, dass der Administrator eine Rolle auswählen muss, um sich auf dem Ziel-IVE anzumelden. (Sie dürfen einen einzelnen Benutzer z. B. nicht mehreren Rollen zuordnen, auch nicht der Rolle des Administrators für die Konfigurationsübertragung, sofern Sie diese Rollen nicht permissiv zusammenführen.) Wir empfehlen das Erstellen eines Kontos, das ausschließlich Administratoren für die Konfigurationsübertragung vorbehalten ist. Dies gewährleistet, dass der Administrator bei der Anmeldung keine Rolle auswählen muss und die Aktionen von Administratoren für die Konfigurationsübertragung in den Protokolldateien eindeutig nachvollzogen werden können.

So übertragen Sie ausgewählte Rollen und Ressourcen von einem IVE auf ein anderes:

1. Erstellen von Administratorkonten auf beiden IVE-Appliances. Anweisungen hierfür finden Sie unter „Konfigurieren der Seite „Delegation““ auf Seite 355. (Siehe die oben aufgeführten Beschränkungen.)
2. Wählen Sie in der Webkonsole die Optionen **Maintenance > Push Config** aus.
3. Geben Sie unter **Target Host Sign-in URL** den Administrator-URL des IVE ein, auf den Rollen und Ressourcenrichtlinien übertragen werden sollen. Beispiel: https://10.10.10.10/admin.
4. Geben Sie den Benutzernamen, das Kennwort und den Authentifizierungsbereich eines Administratorkontos auf dem Ziel-IVE ein, das über volle Administratorberechtigungen verfügt.
5. Aktivieren Sie das Kontrollkästchen **Overwrite duplicate settings**, wenn Sie Benutzerrollen, delegierte Administrationsrollen und Ressourcenrichtlinien auf dem Ziel-IVE überschreiben möchten, die den gleichen Namen wie eine Benutzerrolle, delegierte Administrationsrolle oder Ressourcenrichtlinie auf dem Quell-IVE aufweisen.
6. Aktivieren Sie das Kontrollkästchen **Delegated Admin Roles**, um delegierte Administrationsrollen auf das Ziel-IVE zu kopieren. Gehen Sie dann folgendermaßen vor:
   - Wählen Sie **All roles** aus, um alle delegierten Administrationsrollen auf das Ziel-IVE zu kopieren.
   - Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen auf das Ziel-IVE kopieren möchten.
7. Aktivieren Sie das Kontrollkästchen **User Roles**, um Benutzerrollen auf das Ziel-IVE zu kopieren.
   - Wählen Sie **All roles** aus, um alle delegierten Administratorrollen auf das Ziel-IVE zu kopieren.
   - Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen auf das Ziel-IVE kopieren möchten.
8. Aktivieren Sie das Kontrollkästchen **Resource Policies** , um Ressourcenrichtlinien auf das Ziel-IVE zu kopieren. Aktivieren Sie anschließend die Kontrollkästchen für die Typen von Ressourcenrichtlinien, die Sie kopieren möchten, beispielsweise Richtlinien für Zugriffssteuerung, Zwischenspeicherung oder selektives Neuschreiben.
9. Klicken Sie auf **Push Configuration**, um die ausgewählten Rollen und Ressourcen auf das Ziel-IVE zu kopieren. Das IVE zeigt den Übertragungsstatus unten auf der Seite **Maintenance > Push Config** im Quell-IVE an.

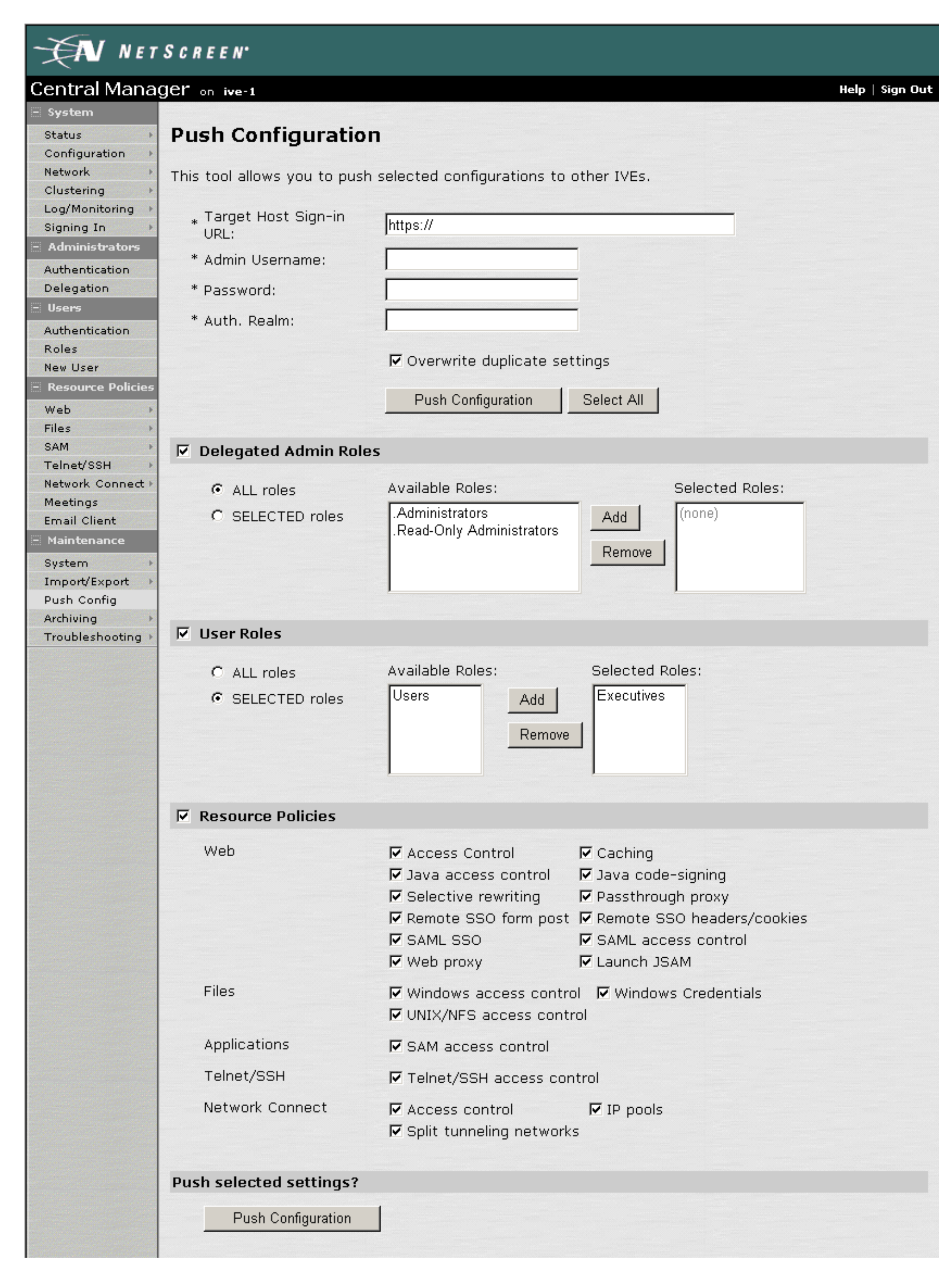


Abbildung 165: Maintenance > Push Config

Konfigurieren der Seite „Archiving“

Die Seite **Maintenance > Archiving** enthält die folgenden Registerkarten:

Auf der Seite **Maintenance > Archiving** können Sie Folgendes durchführen:

Registerkarte „FTP Server“

☑ Planen der Archivierung von Systemdaten auf einem externen FTP-Server

Sie können festlegen, dass Systemprotokolldateien, Konfigurationsdateien und Benutzerkonten täglich oder wöchentlich archiviert werden. Das IVE archiviert die Dateien an den von Ihnen ausgewählten Tagen und Uhrzeiten über FTP auf dem angegebenen Server und in dem angegebenen Verzeichnis. Die Konfigurationsdateien und Benutzerkonten werden verschlüsselt, um eine sichere Übertragung über FTP und eine sichere Speicherung auf anderen Servern zu gewährleisten.

Der Name der Archivdateien enthält, wie nachfolgend dargestellt, das Datum und die Uhrzeit der Archivierung:

- Systemkonfigurationsdateien: `NetScreenConf-`*`Datum-Uhrzeit`*
- Benutzerkonten: `NetScreenUserAccounts-`*`Datum-Uhrzeit`*
- Systemereignisse: `NetScreenccessLog-`*`Datum-Uhrzeit`*
- Administratorereignisse: `NetScreenAdminLog-`*`Datum-Uhrzeit`*
- Benutzerereignisse: `NetScreenEventsLog-`*`Datum-Uhrzeit`*

So legen Sie Archivierungsparameter fest:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Archiving > FTP Server** aus.
2. Geben Sie unter **Archive Settings** den Zielserver, ein Verzeichnis und Ihre FTP-Anmeldeinformationen für diesen Server an. Schließen Sie keine Laufwerksangabe für das Zielverzeichnis ein, beispielsweise: `netscreen/log`.
   - Bei UNIX-Computern geben Sie abhängig vom Basisverzeichnis des Benutzers entweder einen absoluten oder einen relativen Pfad an.
   - Bei Windows-Computern geben Sie einen Pfad an, der relativ zum Ordner `ftproot` ist.
3. Für alle Arten von archivierten Daten geben Sie einen Archivierungsplan an. Für Systemereignisse, Zugriff und Administratorprotokolle können Sie außerdem einen Protokollfilter angeben und den Inhalt der Protokolldatei nach der Archivierung löschen.
4. Klicken Sie auf **Save Changes**.

NETSCREEN

Central Manager on ive-1 — Help | Sign Out

System: Status, Configuration, Network, Clustering, Log/Monitoring, Signing In
Administrators: Authentication, Delegation
Users: Authentication, Roles, New User
Resource Policies: Web, Files, SAM, Telnet/SSH, Network Connect, Meetings, Email Client
Maintenance: System, Import/Export, Push Config, Archiving, Troubleshooting

Archiving To FTP Server

FTP Server | Local Backups

You can schedule automatic archiving of log data, system configuration, and user accounts. To do so, specify an FTP accessible location for the data, an FTP account to use, and the specific schedule for each type of archived data.

Archive Settings

Archive Server: ______ Name or IP address
Destination Directory: ______
FTP Username: ______
FTP Password: ______

Archive Schedule

Select one or more components to schedule an archive.

☑ **Archive events log**
Use this filter: WELF: WELF
Sun Mon Tue Wed Thu Fri Sat — ○ Every hour (00:00am till 11:00pm) — ◉ Specified Time: 00:00 AM
☐ Clear log after archiving

☑ **Archive user access log**
Use this filter: WELF: WELF
Sun Mon Tue Wed Thu Fri Sat — ○ Every hour (00:00am till 11:00pm) — ◉ Specified Time: 00:00 AM
☐ Clear log after archiving

☑ **Archive admin access log**
☐ Clear log after archiving

☑ **Archive system configuration**
Sun Mon Tue Wed Thu Fri Sat — ○ Every hour (00:00am till 11:00pm) — ◉ Specified Time: 00:00 AM
You can password-protect the archived configuration files. If you do so, the password will need to be provided to import them.
Password for configuration file: ______

☑ **Archive user accounts**
Sun Mon Tue Wed Thu Fri Sat — ○ Every hour (00:00am till 11:00pm) — ◉ Specified Time: 00:00 AM
You can password-protect the archived configuration files. If you do so, the password will need to be provided to import them.
Password for configuration file: ______

Abbildung 166: **Maintenance > Archiving > FTP Server**

Registerkarte „Local Backups“

☑ Speichern eines Snapshots der aktuellen Konfiguration

Mit den Central Manager-Appliances für Access Series und Meeting Series können Snapshots der aktuellen Systemkonfiguration und Benutzerkonten direkt im IVE gespeichert werden. Mithilfe dieser Konfigurationen können das IVE oder IVE-Cluster in dem Zustand wiederhergestellt werden, der in der verschlüsselten Datei enthalten ist. Beachten Sie, dass diese Dateien nur Konfigurationsinformationen und keine Protokolle enthalten.

Sie können auf dem IVE bis zu fünf Snapshots der Systemkonfiguration sowie fünf Snapshots von Benutzerkonten speichern. Wenn Sie diese Zahl überschreiten, überschreibt das IVE den ältesten Snapshot mit dem neuen Snapshot. Wenn der älteste Snapshot nicht überschrieben werden soll, müssen Sie vor dem Speichern des neuesten Snapshots einen anderen Snapshot auswählen, der gelöscht werden soll.

So speichern Sie die aktuelle Systemkonfiguration:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Archiving > Local Backups** aus.
2. Klicken Sie auf **Save Configuration** oder **Save User Accounts**. Das IVE fügt der Liste einen neuen Snapshot hinzu und benennt ihn mit dem aktuellen Datum und der aktuellen Uhrzeit.

☑ Wiederherstellen des System- oder Benutzerkontenstatus aus einem Snapshot

System- und Benutzersnapshots können verwendet werden, um ein einzelnes IVE oder einen IVE-Cluster zu aktualisieren. Wenn Sie ein IVE wiederherstellen möchten, das Teil eines Clusters ist, überträgt das IVE die Konfiguration automatisch auf alle anderen Clustermitglieder. Der Cluster bleibt solange deaktiviert, bis die Einstellungen aller Clustermitglieder mithilfe der Snapshotkonfiguration aktualisiert wurden. Starten Sie den Cluster dann neu, und aktivieren Sie ihn.

So überschreiben Sie die Konfiguration mit Einstellungen aus einer Sicherungsdatei:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Archiving > Local Backups** aus.
2. Aktivieren Sie das Kontrollkästchen neben der Sicherungsdatei für die Systemkonfiguration oder das Benutzerkonto, die zum Wiederherstellen des Systems verwendet werden soll.
3. Wenn Sie eine Systemkonfiguration wiederherstellen, müssen Sie angeben, ob dabei auch das Zertifikat, die IP-Adresse und die Netzwerkeinstellungen aus der Konfigurationsdatei übernommen werden sollen. Beachten Sie bei der Aktualisierung Folgendes:
   - **Access Series FIPS-System** – Wenn Sie ein Zertifikat importieren möchten, müssen Sie ein Zertifikat mit einem FIPS-kompatiblen privaten Schlüssel auswählen. Um FIPS-Kompatibilität zu gewährleisten, wählen Sie ein Zertifikat und die zugehörigen privaten Security World-Schlüssel aus, die auf einem Access Series FIPS-System erzeugt wurden.
   - **Gesamter Cluster** – Gehen Sie beim Einschließen von Netzwerkeinstellungen vorsichtig vor. Da IP-Adressen und andere Einstellungen wahrscheinlich nicht für alle Mitglieder des Clusters gelten, könnte die Kommunikation zwischen den Mitgliedern unterbrochen werden, nachdem die Einstellungen auf alle Mitglieder übertragen wurden.
4. Klicken Sie auf **Restore**. Die Änderungen werden erst nach einem Neustart des IVE wirksam. Anschließend müssen Sie sich erneut am IVE anmelden, um auf die Webkonsole zugreifen zu können.

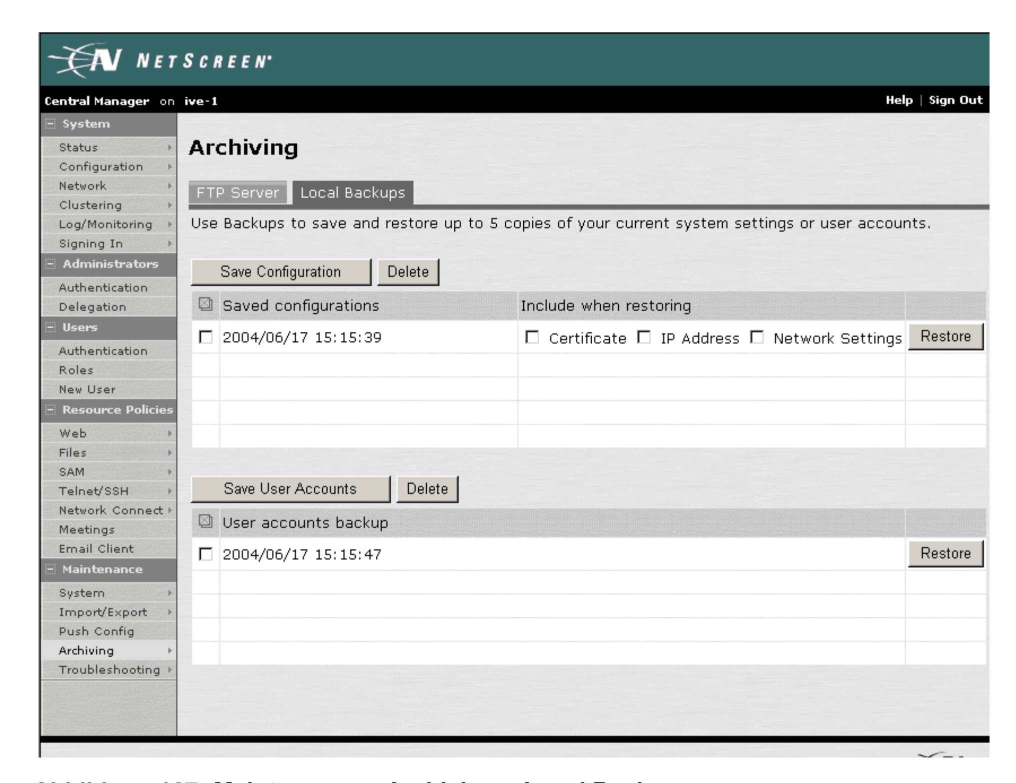


Abbildung 167: **Maintenance > Archiving > Local Backups**

Konfigurieren der Seite „Troubleshooting“

Die Seite **Maintenance >Troubleshooting** enthält die folgenden Registerkarten:

Auf der Seite **Maintenance > Troubleshooting** können Sie Folgendes durchführen:

Registerkarte „User Sessions > Simulation“

☑ **Simulieren einer Benutzersitzung**

Mit dieser Registerkarte können Sie Probleme lösen, indem Sie die Ereignisse simulieren, die das Problem verursachen. Mithilfe der Registerkarte **Simulation** können Sie virtuelle Benutzersitzungen erstellen, wobei sich die Endbenutzer nicht beim IVE anmelden und die entsprechenden Probleme reproduzieren müssen. Außerdem können Sie die Registerkarte **Simulation** auch verwenden, um neue Authentifizierungs- und Autorisierungsrichtlinien vor der Verwendung in einer Produktionsumgebung zu testen.

Damit Sie die Simulation verwenden können, müssen Sie die zu simulierenden Ereignisse angeben. (Sie können z. B. eine virtuelle Sitzung erstellen, in der sich „John Doe" über einen Netscape-Browser um 6:00 Uhr am Bereich „Users" anmeldet.) Anschließend müssen Sie angeben, welche Ereignisse in der Simulation aufgezeichnet und protokolliert werden sollen. Sie können drei Haupttypen von Ereignissen im Simulationsprotokoll aufzeichnen:

- **Pre-Authentication**

  Das IVE simuliert Authentifizierungs-Vorabprüfungen auf der Bereichs- und Rollenebene für den virtuellen Benutzer und zeichnet die daraus resultierenden Protokollmeldungen im Simulationsprotokoll auf.

- **Role Mapping**

  Das IVE simuliert Rollenzuordnungsprüfungen, ermittelt die für die Simulation zu verwendende Rolle auf Grundlage der Rollenzuordnungsregeln und zeichnet die daraus resultierenden Protokollmeldungen im Simulationsprotokoll auf.

- **Ressourcenrichtlinien**

  Das IVE simuliert die Verarbeitung von Ressourcenrichtlinien für den virtuellen Benutzer und zeichnet die daraus resultierenden Protokollmeldungen im Simulationsprotokoll auf.

So simulieren Sie eine Benutzersitzung:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > User Sessions > Simulation** aus.
2. Geben Sie im Feld **Query Name** einen Namen für die Abfrage ein.
3. Geben Sie im Feld **Username** den Benutzernamen des IVE-Benutzers ein, für den Sie eine Simulation ausführen möchten. Beachten Sie, dass Sie anstelle eines Benutzernamens auch einen Platzhalter (*) verwenden können. Wenn sich die Benutzer beispielsweise an einem anonymen Server anmelden, kann es ratsam sein, den Platzhalter (*) zu verwenden, da Sie den internen Benutzernamen, der dem Benutzer vom IVE zugewiesen wird, nicht kennen.
4. Wählen Sie im Dropdownmenü **Realm** den Bereich des IVE-Benutzers aus, für den Sie eine Simulation ausführen möchten.

5. Wenn Sie ermitteln möchten, ob das IVE einen bestimmten Ressourcenrichtlinientyp auf eine Benutzersitzung anwendet, gehen Sie folgendermaßen vor:
   - Geben Sie im Feld **Resource** die Ressource ein, die Sie simulieren möchten.
   - Wählen Sie in der Dropdownliste **Resource** einen Richtlinientyp aus.
   - Legen Sie die zu protokollierenden Richtlinientypen mithilfe der Kontrollkästchen im Abschnitt **Events to Log** fest.

   Wenn Sie z. B. testen möchten, ob ein Benutzer auf die Yahoo-Website zugreifen kann, geben Sie im Feld **Resource** die Zeichenfolge „http://www.yahoo.com" ein. Wählen Sie dann in der Dropdownliste den Eintrag **Web** aus, und aktivieren Sie im Abschnitt **Events to Log** das Kontrollkästchen **Access**.
6. Wenn Sie ermitteln möchten, ob sich ein Benutzer erfolgreich beim IVE anmelden kann, aktivieren Sie das Kontrollkästchen **Pre-Authentication**.
7. Um zu ermitteln, ob einem Benutzer eine bestimmte Rolle zugeordnet werden kann, aktivieren Sie das Kontrollkästchen **Role Mapping**. Beachten Sie, dass mit dieser Option gesteuert wird, ob die Ergebnisse der Rollenzuordnung im Simulationsprotokoll aufgezeichnet werden. Es wird jedoch nicht gesteuert, ob das IVE Rollenzuordnungsregeln ausführt. Das IVE führt grundsätzlich Rollenzuordnungsregeln aus, unabhängig davon, ob Sie dieses Kontrollkästchen aktivieren oder deaktivieren.
8. Verwenden Sie im Abschnitt **Variables** eine Kombination aus Text und Variablen, um einen benutzerdefinierten Ausdruck zu erstellen, der genau dieselben Werte wie in der tatsächlichen Sitzung des Benutzers widerspiegelt, bei dem ein Problem aufgetreten ist. Wenn Sie beispielsweise eine Sitzung erstellen möchten, in der sich der Benutzer um 6:00 Uhr beim IVE anmeldet, geben Sie im Feld **Variables** Folgendes ein: „time = 6:00 AM". Umfassende Anweisungen zum Erstellen eines benutzerdefinierten Ausdrucks finden Sie in Anhang Anhang D.: auf Seite 595. Sie können auch die Syntax für eine bestimmte Variable anzeigen, indem Sie in **Variables Dictionary** auf den Pfeil neben der entsprechenden Variable klicken.

Wichtig: Wenn Sie keinen benutzerdefinierten Ausdruck erstellen können, der die IP-Adresse des virtuellen Benutzers umfasst, verwendet das IVE stattdessen Ihre aktuelle IP-Adresse. Darüber hinaus sollten Sie beachten, dass das IVE bei Verwendung der Rollenvariable zum Angeben der Rolle des virtuellen Benutzers (z. B. role="Users") die Ergebnisse der Rollenzuordnungsregeln ignoriert und den virtuellen Benutzer den von Ihnen angegebenen Rollen zuweist.

---

9. Wählen Sie eine der folgenden Optionen aus:
   - **Run Simulation** – Führt die angegebene Simulation aus und erstellt eine Bildschirmprotokolldatei.
   - **Save Query** – Speichert die Abfrage.
   - **Save Query and Run Simulation** – Führt die angegebene Simulation aus und speichert sie für eine spätere Verwendung.
10. Wählen Sie nach dem Ausführen der Simulation die Option **Save Log As** aus, um die Ergebnisse der Simulation in einer Textdatei zu speichern.

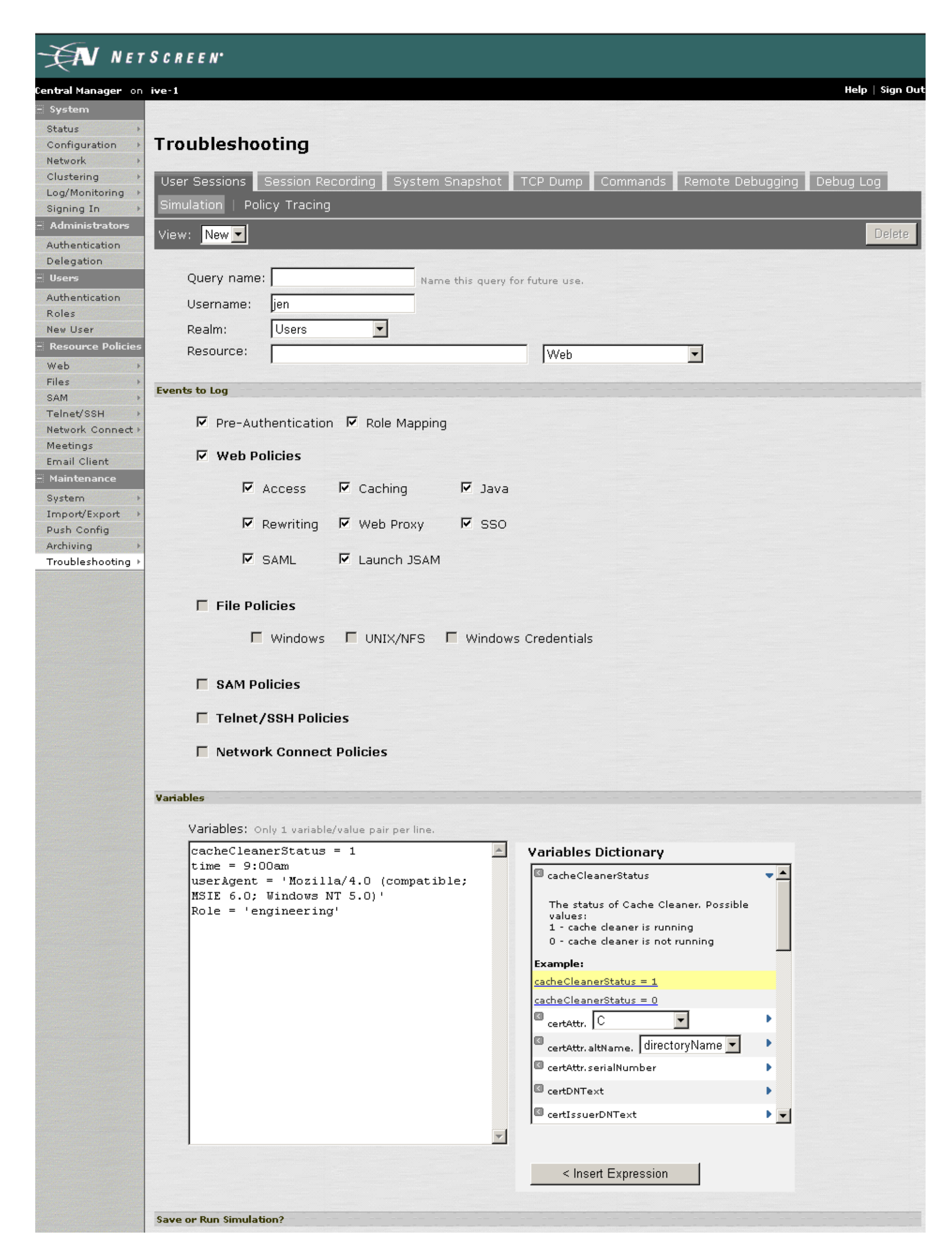


Abbildung 168: **Maintenance > Troubleshooting > User Session > Simulation**

Registerkarte „User Sessions > Policy tracing“

Mit dieser Registerkarte können Sie Probleme beheben, indem Sie die Ereignisse bei der Anmeldung eines Benutzers an einem Bereich verfolgen. Wenn Sie eine Richtlinienverfolgungsdatei für einen einzelnen Benutzer aufzeichnen, zeigt das IVE Protokolleinträge an, in denen die Aktionen des Benutzers sowie Angaben zu den Gründen aufgeführt sind, aus denen diesem Benutzer der Zugriff auf verschiedene Funktionen (wie das Zugreifen auf das Web oder auf einen Dateiserver) gewährt oder verweigert wird.

Sie können beispielsweise einen Bereich „Human Resources" (Personalabteilung) mit zwei Rollenzuordnungsregeln erstellen:

- **All Employees**

  In dieser Rolle ermöglichen Sie nur Webbrowsing. Benutzer werden der Rolle mithilfe der folgenden Regel zugeordnet: if username = *, map to „All Employees". Jeder Benutzer, der sich an diesem Bereich anmelden darf, wird also automatisch der Rolle „All Employees" zugeordnet.

- **Human Resources Staff**

  Für diese Rolle ermöglichen Sie die Web-, Datei- und Konferenzfunktionen. Benutzer werden der Rolle mithilfe der folgenden Regel zugeordnet: if LDAP group=human resources, map to „Human Resources Staff." Ein Benutzer muss also der Gruppe „Human Resources" auf dem LDAP-Authentifizierungsserver angehören, um der Rolle zugeordnet werden zu können.

Sie vermuten möglicherweise, dass Joe beiden Rollen angehört. Nach der Anmeldung am IVE kann er jedoch nicht auf die Dateinavigationsfunktionen und die Secure Meeting-Funktionen zugreifen, die in der Rolle „Human Resources Staff" aktiviert sind. Wenn Sie die Richtlinienverfolgung aktivieren, um zu ermitteln, aus welchen Gründen Joe nicht auf alle erwarteten Funktionen zugreifen kann, könnten beispielsweise die folgenden Protokolleinträge angezeigt werden:

Severity	ID	Message
Info	PTR10103	2004/01/28 17:52:40 - ive-2 - [10.12.254.193] admin03(Admin Users)[.Administrators] - joe:human resources realm - Policy Tracing turned on
Info	PTR22787	2004/01/28 17:53:12 - ive-2 - [10.12.254.193] joe(human resources realm) - Successful authentication with auth server 'human resources server'
Info	PTR10209	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Realm human resources realm running 2 mapping rules for user joe
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable user = "joe"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable sourceIp = 10.12.254.193
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable userAgent = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable loginTime = Wed Jan 28 17:53:12 2004
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable networkIf = "internal"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable realm = "human resources realm"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable auth = "human resources server"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable hostCheckerPolicy =
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable cacheCleanerStatus = 0
Info	PTR10212	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Mapped to roles All Employees by rule 'user = "*"'
Info	PTR10218	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - No match on rule 'group.humanresources'
Info	PTR10218	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - No match on rule 'group.humanresources'
Info	PTR10205	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Realm human resources realm mapped user joe to roles All Employees

Abbildung 169: **Maintenance > Troubleshooting > User Session > Policy Tracing > Policy Trace File**

Beim Durchgehen der Verfolgungsdatei sehen Sie, dass das Problem in Eintrag `PTR10218` liegt:

```
joe(human resources realm) - No match on rule
'group.humanresources'
```

Dieser Eintrag zeigt, dass das IVE Joe nicht der Rolle „Human Resource Staff" zugeordnet hat, weil er kein Mitglied der Gruppe „Human Resources" auf dem LDAP-Server ist.

☑ Aufzeichnen einer Richtlinienverfolgungsdatei

Verwenden Sie diese Registerkarte, wenn die Benutzer Probleme beim Zugreifen auf Funktionen feststellen, die sie normalerweise im Rahmen ihrer jeweiligen Rollen verwenden können. Mithilfe der in der Richtlinienverfolgungsdatei protokollierten Ereignisse können Sie diese Probleme diagnostizieren. Beachten Sie, dass Benutzerzugriffsprotokolle nur für die unter **Events to Log** aktivierten Richtlinien protokolliert werden.

So erstellen Sie eine Richtlinienverfolgungsdatei:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > User Sessions > Policy Tracing** aus.

2. Geben Sie im Feld **User** den IVE-Benutzernamen des Benutzers ein, den Sie verfolgen möchten. Beachten Sie, dass Sie anstelle eines Benutzernamens auch einen Platzhalter (*) verwenden können. Wenn sich die Benutzer beispielsweise an einem anonymen Server anmelden, kann es ratsam sein, den Platzhalter (*) zu verwenden, da Sie den internen Benutzernamen, der dem Benutzer vom IVE zugewiesen wird, nicht kennen.
3. Wählen Sie im Feld **Realm** den Bereich des Benutzers aus. Beachten Sie, dass auf dem IVE kein Bereich ausgewählt werden kann, der einem anonymen Authentifizierungsserver zugeordnet ist.
4. Aktivieren Sie unter **Events to log** die Ereignistypen, die in der Protokolldatei für die Richtlinienverfolgung erfasst werden sollen.
5. Klicken Sie auf **Start Recording**. Bitten Sie den Benutzer nach dem Beginn der Aufzeichnung, sich am IVE anzumelden.
6. Klicken Sie zum Anzeigen der Protokolleinträge auf **View Log**.
7. Klicken Sie auf **Stop Recording**, wenn Sie genügend Informationen erfasst haben.
8. Gehen Sie die Meldungen in der Protokolldatei durch, um den Grund für das abweichende Verhalten zu finden. Wenn Sie das Problem nicht erkennen und beheben können, klicken Sie auf **Save Log As**, um eine Kopie der Protokolldatei im Netzwerk zu speichern. Senden Sie die Datei anschließend zur Überprüfung an den Juniper Networks-Support.
9. Klicken Sie auf **Clear Log**, um den Inhalt der Protokolldatei zu löschen, oder auf **Delete Trace**, um den Inhalt der Protokolldatei zu löschen und die Standardeinträge aus den Feldern für Benutzername und Bereich zu entfernen.

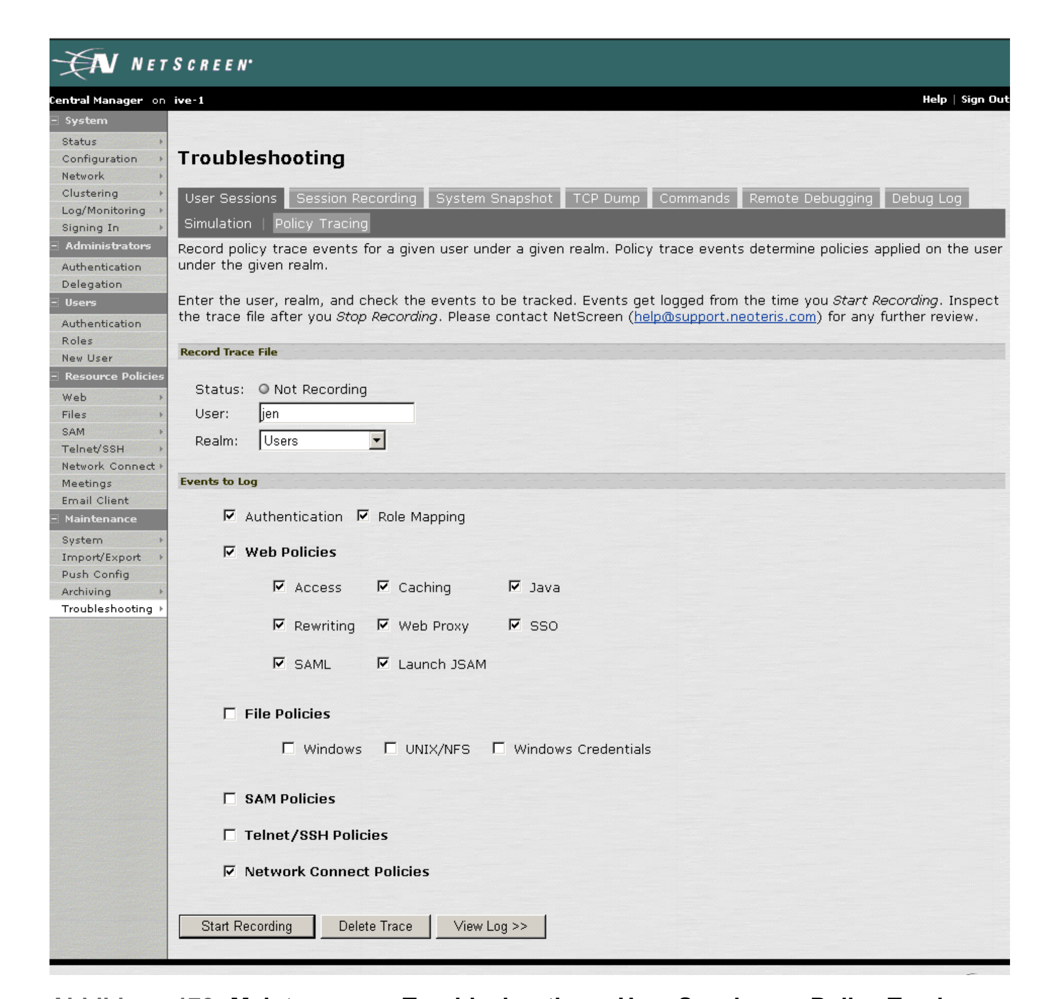


Abbildung 170: **Maintenance > Troubleshooting > User Sessions > Policy Tracing**

Registerkarte „Session Recording“

☑ Aufzeichnen einer Ablaufverfolgungsdatei zu Debuggingzwecken

Auf dieser Registerkarte können Sie eine Ablaufverfolgungsdatei aufzeichnen, in der die Aktionen eines Benutzers beim Navigieren zu einer Website aufgeführt werden, die über das IVE nicht ordnungsgemäß angezeigt wird. Wenn Sie diese Option verwenden, erzwingt das IVE eine erneute Anmeldung des angegebenen Benutzers und beginnt dann mit der Aufzeichnung sämtlicher Benutzeraktionen. Beachten Sie, dass das IVE den Benutzer über die Aufzeichnung der Benutzeraktionen benachrichtigt.

So zeichnen Sie eine Ablaufverfolgungsdatei auf:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Session Recording** aus.
2. Geben Sie den Benutzernamen des entsprechenden Benutzers ein.
3. Aktivieren Sie das Kontrollkästchen **Ignore browser cache**, um diese Zusatzinformationen aus der Aufzeichnung auszuschließen (optional).
4. Klicken Sie auf **Start Recording**.
5. Weisen Sie den Benutzer an, zu der problematischen Website zu navigieren.
6. Klicken Sie auf **Stop Recording**.
7. Klicken Sie auf **dsrecord.log**, um die Datei auf einen Netzwerkcomputer herunterzuladen. Entfernen Sie alle vertraulichen Daten mithilfe eines Text-Editors.
8. Senden Sie die Datei zur Überprüfung per E-Mail an den Juniper Networks-Support.

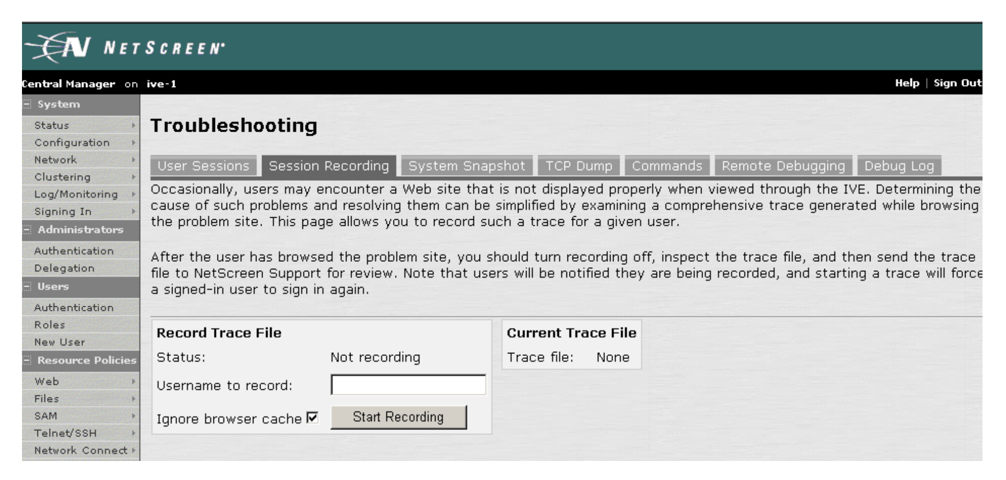


Abbildung 171: **Maintenance > Troubleshooting > Session Recording**

Registerkarte „System Snapshot“

☑ Erstellen eines Snapshots des IVE-Systemstatus

Erstellen Sie auf dieser Registerkarte einen Snapshot des IVE-Systemstatus. Wenn Sie diese Option verwenden, führt das IVE verschiedene Dienstprogramme aus, um Details zum IVE-Systemstatus zu erfassen, beispielsweise zum belegten Speicherplatz, zur Auslagerungsleistung, zur Anzahl der ausgeführten Prozesse, zur Systembetriebszeit, zur Anzahl der geöffneten Dateibeschreibungen, zu den verwendeten Ports und zu den Access Series FIPS-Protokollmeldungen. Das IVE speichert bis zu zehn Snapshots, die in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei abgelegt werden. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den Juniper Networks-Support senden.

So erstellen Sie einen Snapshot des IVE-Systemstatus:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > System Snapshot** aus.
2. Aktivieren Sie das Kontrollkästchen **Include system config**, um Informationen zur Systemkonfiguration in den Snapshot einzuschließen (optional).
3. Aktivieren Sie das Kontrollkästchen **Include and clear debuglog**, um die mithilfe der Registerkarte **Debug Log** (Seite 562) erstellte Protokolldatei in den Systemsnapshot einzuschließen.

4. Klicken Sie auf **Take Snapshot**.
5. Wenn das IVE das Erstellen des Snapshots beendet hat, klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.
6. Senden Sie die Datei zur Überprüfung per E-Mail an den Juniper Networks-Support.
7. Klicken Sie abschließend zum Löschen des Snapshots auf **Delete**.

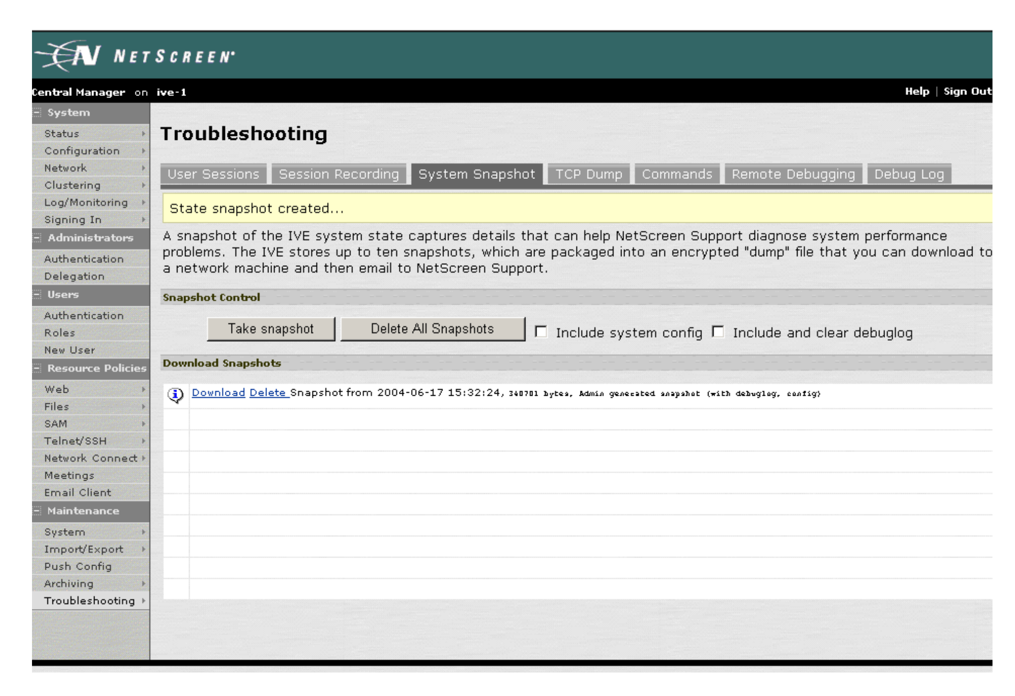


Abbildung 172: **Maintenance > Troubleshooting > System Snapshot**

Registerkarte „TCP Dump“

☑ Sniffing von Netzwerkpaketheadern

Auf dieser Registerkarte können Sie Sniffing von Netzwerkpaketheadern durchführen und die Ergebnisse in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei speichern. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den Juniper Networks-Support senden.

So führen Sie Sniffing von Netzwerkpaketheadern durch:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > TCP Dump** aus.
2. Wählen Sie den IVE-Port aus, an dem Sniffing von Netzwerkpaketheadern durchgeführt werden soll.
3. Deaktivieren Sie den **Promiscuous**-Modus, sodass Sniffing nur für Pakete durchgeführt wird, die für das IVE bestimmt sind.
4. Klicken Sie auf **Start Sniffing**.
5. Klicken Sie auf **Stop Sniffing**, um das Sniffing zu beenden und eine verschlüsselte Datei zu erstellen.
6. Klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.
7. Senden Sie die Datei zur Überprüfung per E-Mail an den Juniper Networks-Support.

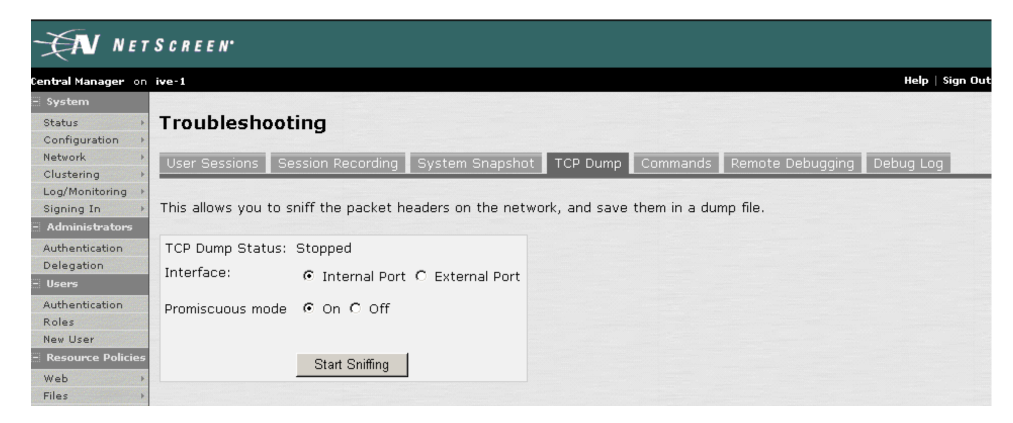


Abbildung 173: **Maintenance > Troubleshooting > TCP Dump (Erstellen einer Dumpdatei)**

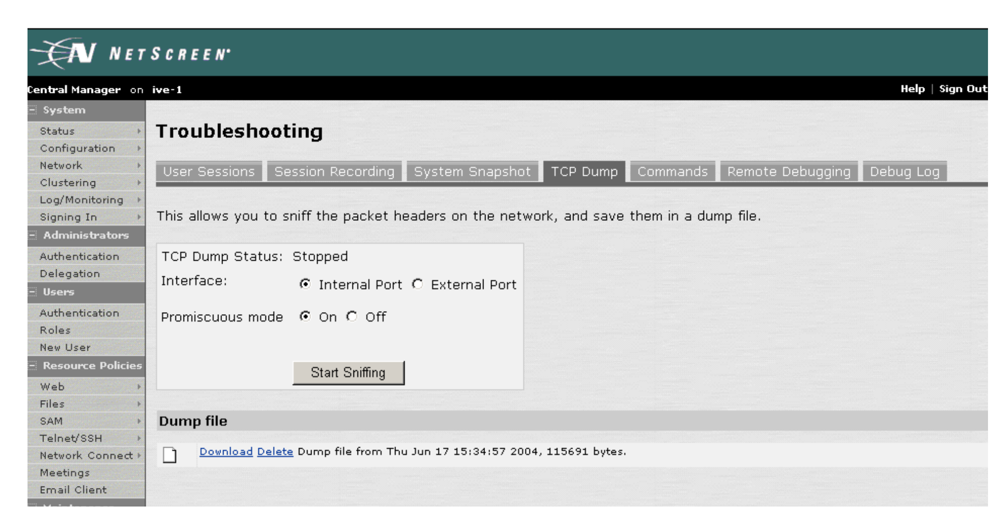


Abbildung 174: **Maintenance > Troubleshooting > TCP Dump (nach Erstellen einer Dumpdatei)**

Registerkarte „Commands“

☑ Ausführen eines ARP-, ping-, traceroute- oder nslookup-Befehls

Auf dieser Registerkarte können Sie UNIX-Befehle ausführen, um die IVE-Netzwerkverbindung zu testen.

So führen Sie einen UNIX-Befehl aus, um die IVE-Netzwerkverbindung zu testen:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Commands** aus.
2. Wählen Sie in der Liste **Command** den Befehl aus, der ausgeführt werden soll.
3. Geben Sie im Feld **Target Server** die IP-Adresse des Zielservers ein.
4. Klicken Sie zur Ausführung des Befehls auf **OK**.

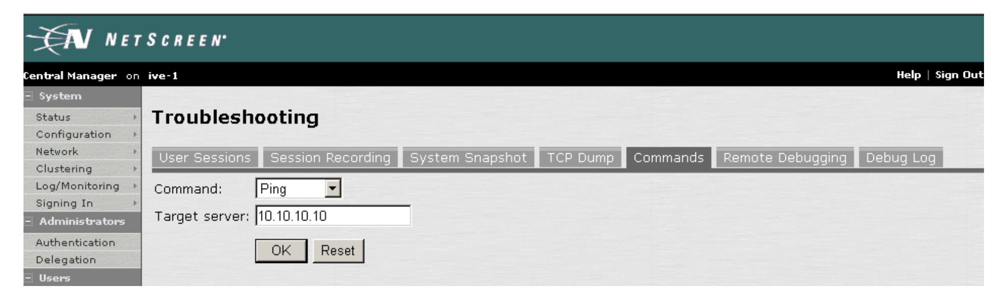


Abbildung 175: **Maintenance > Troubleshooting > Commands**

Registerkarte „Remote Debugging“

☑ Aktivieren von Remotedebugging für den Juniper Networks-Support

Auf dieser Registerkarte können Sie es dem Juniper Networks-Support-Team ermöglichen, auf Ihrem Produktions-IVE Debuggingtools auszuführen. Zur Aktivierung dieser Option müssen Sie mit dem Juniper Networks-Support zusammenarbeiten, um einen Debuggingcode sowie einen Host zu erhalten, mit dem das IVE die Verbindung herstellt.

So aktivieren Sie Remotedebugging:

1. Wenden Sie sich an den Juniper Networks-Support, um die Bedingungen für eine Remotedebuggingsitzung einzurichten.
2. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Remote Debugging** aus.
3. Geben Sie den Debuggingcode ein, der vom Juniper Networks-Support zur Verfügung gestellt wurde.
4. Geben Sie den Hostnamen ein, der vom Juniper Networks-Support zur Verfügung gestellt wurde.
5. Klicken Sie auf **Enable Debugging**, sodass das Juniper Networks-Support-Team auf das IVE zugreifen kann.
6. Teilen Sie dem Juniper Networks-Support mit, dass auf Ihr IVE zugegriffen werden kann.
7. Klicken Sie auf **Disable Debugging**, wenn der Juniper Networks-Support Ihnen mitteilt, dass die Remotedebuggingsitzung beendet ist.

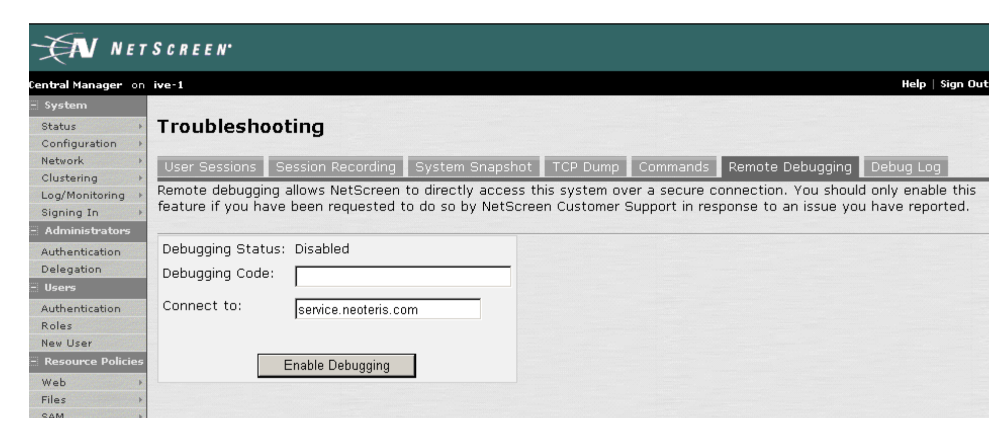


Abbildung 176: **Maintenance > Troubleshooting > Remote Debugging**

Registerkarte „Debug Log“

☑ Aktivieren des Debugprotokolls

Verwenden Sie die Registerkarte **Debug Log**, um ein Debugprotokoll zu erstellen, das Sie an den Juniper Networks-Support senden können. Verwenden Sie diese Registerkarte nur, wenn Sie vom Support dazu aufgefordert werden.

So aktivieren Sie das Debugprotokoll:

1. Wählen Sie in der Webkonsole die Optionen **Maintenance > Troubleshooting > Remote Debugging** aus.
2. Aktivieren Sie das Kontrollkästchen **Debug Logging On**.
3. Geben Sie die Protokollgröße, die Detailebene und den vom Juniper Networks-Support angegebenen Ereigniscode ein.
4. Wählen Sie die Registerkarte **Maintenance > Troubleshooting > System Snapshot** aus.
5. Aktivieren Sie das Kontrollkästchen **Include and clear debuglog**.
6. Klicken Sie auf **Take snapshot**, um eine Datei mit dem Debugprotokoll zu erstellen.
7. Klicken Sie auf **Download**.
8. Fügen Sie die Snapshotdatei an eine E-Mail-Nachricht an, und senden Sie diese an den Juniper Networks-Support.

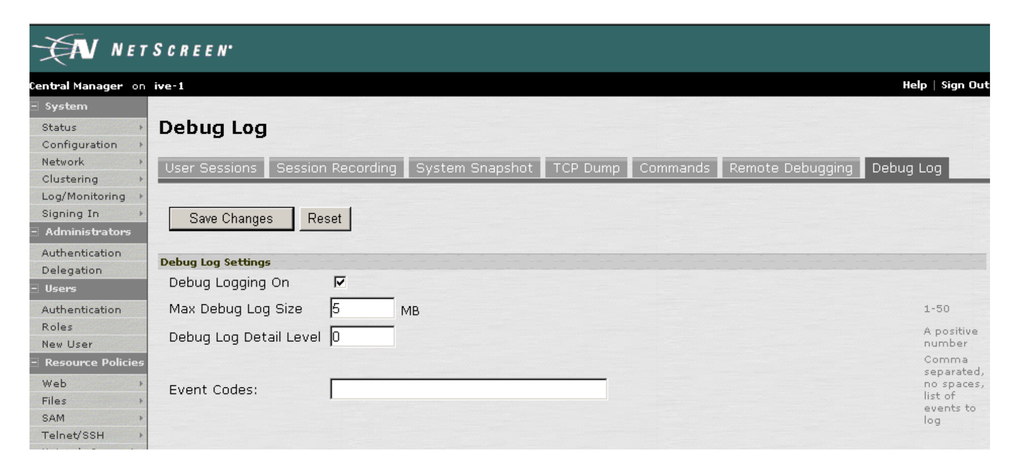


Abbildung 177: **Maintenance > Troubleshooting > Debug Log**

Teil 4
Zusatzinformationen

In diesem Abschnitt finden Sie weiterführende Informationen zur Konfiguration von Access Series-Produkten.

Inhalt

Anhang A.
Verwenden der seriellen Konsole des IVE

Die serielle Konsole des IVE bietet eine Oberfläche zum Durchführen der folgenden Vorgänge:

☑ Herstellen einer Verbindung mit der seriellen Konsole des IVE

Um Aufgaben über die serielle Konsole von IVE durchführen zu können, müssen Sie ein Konsolenterminal oder einen Laptop an das IVE-Gerät anschließen.

So stellen Sie eine Verbindung mit der seriellen Konsole des IVE her:

1. Schließen Sie ein Nullmodem-Crossover-Kabel vom Konsolenterminal oder Laptop an das IVE-Gerät an. Dieses Kabel ist im Lieferumfang des Geräts enthalten. Verwenden Sie kein einfaches serielles Kabel.
2. Konfigurieren Sie das Terminal oder die Terminalemulationssoftware (beispielsweise HyperTerminal) mit den folgenden Parametern für serielle Verbindungen:
   - 9600 Bit pro Sekunde
   - 8 Bit, keine Parität (8N1)
   - 1 Stopp-Bit
   - Keine Flusskontrolle

3. Drücken Sie die **Eingabetaste**, bis die serielle Konsole von IVE angezeigt wird.

Hinweis: Wenn Sie ein Access Series FIPS-Gerät betreiben und zum ersten Mal eine Verbindung mit der seriellen Konsole herstellen, müssen Sie zudem den Modusschalter des Kryptographiemoduls auf I (Initialisierungsmodus) stellen.

```
C:\WINNT\system32\telnet.exe

Welcome to the NetScreen Serial Console!

Current version: 4.1.41-latest.daily.0607.1 (build 6454)
Rollback version: 4.0.v40.p1 (build 5858)
Reset version: 4.0.v40.p1 (build 5858)

   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log
   4. Reboot/Shutdown/Restart this IVE
   5. toggle password protection for the console (Off)
   6. Create a Super Admin session.
   7. Replace Administrator Card Set
Choice: _
```

Abbildung 178: **IVE Serielle Konsole**

☑ Rollback zu einem vorherigen Systemzustand

Sie können das IVE-System normalerweise über die Webkonsole folgendermaßen in einen vorherigen Systemzustand zurückversetzen:

1. Navigieren Sie zu den zuvor gespeicherten System- und Benutzerkonfigurationsdateien, in denen die gewünschten Daten gespeichert sind.
2. Laden Sie das gewünschte Serverpaket von der Juniper Networks-Supportsite herunter.
3. Importieren Sie das gewünschte Serverpaket.
4. Importieren Sie die gewünschten System- und Benutzerkonfigurationsdateien.

   Der IVE speichert die aktuellen Systemkonfigurationsinformationen und die des vorherigen Systemzustands. Wenn Sie das Serverpaket aktualisieren und Ihr Gerät in den vorherigen Zustand zurücksetzen möchten, empfehlen wir Ihnen, den zuvor aufgeführten Anweisungen zu folgen. Wenn Sie nicht auf die Webkonsole zugreifen können, stellen Sie eine Verbindung mit der seriellen Konsole her, um ein Rollback zum vorherigen Systemzustand durchzuführen.

Wenn Sie bisher noch keine Serveraktualisierung durchgeführt haben, gibt es keinen älteren Systemzustand, und die Option ist daher nicht verfügbar. Wenn Sie eine Serveraktualisierung durchgeführt haben, gehen alle System- und Benutzerkonfigurationsdaten, die nach der Aktualisierung erstellt wurden, verloren. Dies vermeiden Sie, indem Sie die aktuellen Konfigurationsdateien vor dem Rollback des Systems exportieren und anschließend wieder importieren.

Ein Rollback zu einem vorherigen Systemzustand ist auch über die Webkonsole möglich, wie unter „Installieren eines Juniper Networks-Softwaredienstpakets“ auf Seite 526 beschrieben.

Hinweis: Wenn Sie ein Access Series FIPS-Gerät betrieben und ein Rollback zu einer vorherigen Security World vornehmen möchten, folgen Sie den Anweisungen unter „Wiederherstellen einer archivierten Security World (nur Access Series FIPS)“ auf Seite 576.

So führen Sie ein Rollback zum vorherigen Serverzustand durch:

1. Stellen Sie eine Verbindung mit der seriellen Konsole her (Seite 567).
2. Melden Sie sich in einem Browserfenster an der Webkonsole an.
3. Wählen Sie **Maintenance > System > Platform** aus.
4. Klicken Sie auf **Reboot Now**, und wechseln Sie dann wieder zum Konsolenprogrammfenster zurück. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.
5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tab-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie `rollback` ein, und drücken Sie dann die **Eingabetaste**.

```
LI

Hit [Tab] for choices, or wait for auto load.
Choose configuration to load:
current          rollback        factory-reset

Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: rollback_
```

Abbildung 179: IVE Serielle Konsole
Nach dem Klicken auf „Reboot Now“ auf der Seite Maintenance > System > Platform.

Hinweis:

- Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zurück in die Webkonsole wechseln und auf **Reboot Now** klicken, um den Vorgang erneut zu starten.
- Wenn Sie bereits ein Systemrollback durchgeführt haben, ist die Rollbackoption erst wieder verfügbar, wenn Sie die Serversoftware erneut aktualisieren.

Der Rollbackstatus des Servers wird auf den Bildschirm ausgegeben. Wenn der Vorgang abgeschlossen ist, werden Sie zum Drücken der **Eingabetaste** aufgefordert, um die Systemeinstellungen zu ändern. Dadurch kehren Sie zu den Optionen für das erste Setup zurück. Wenn Sie die Dateneingabe abgeschlossen haben, schließen Sie einfach das Programmfenster.

☑ Zurücksetzen des IVE-Geräts auf die Werkseinstellungen

Es kann im Ausnahmefall erforderlich sein, das IVE-Gerät auf die Werkseinstellungen zurückzusetzen. Bevor Sie diese tief greifende Systemwiederherstellungsoption ausführen, sollten Sie sich an den Juniper Networks-Support wenden. Vor dem Zurücksetzen auf die Werkseinstellungen sollten Sie nach Möglichkeit die aktuellen System- und Benutzerkonfigurations-daten exportieren.

So setzen Sie das Gerät auf die Werkseinstellungen zurück:

1. Stellen Sie eine Verbindung mit der seriellen Konsole her (Seite 567).
2. Melden Sie sich in einem Browserfenster an der Webkonsole an.
3. Wählen Sie **Maintenance > System > Platform** aus.
4. Klicken Sie auf **Reboot Now**, und wechseln Sie dann wieder zum Konsolenprogrammfenster zurück. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.
5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tab-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie `factory-reset` ein, und drücken Sie dann die **Eingabetaste**.

```
LI

Hit [Tab] for choices, or wait for auto load.
Choose configuration to load:
current          factory-reset

Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: factory-reset
Loading factory-reset...........
```

Abbildung 180: IVE Serielle Konsole
Nach dem Klicken auf „Reboot Now“ auf der Seite Maintenance > System > Platform.

Hinweis: Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zurück in die Webkonsole und auf **Reboot Now** klicken, um den Vorgang erneut zu starten.

---

6. Wenn Sie aufgefordert werden, das Zurücksetzen auf die Werkseinstellungen zu bestätigen, geben Sie `proceed` ein, und drücken Sie dann die **Eingabetaste**.

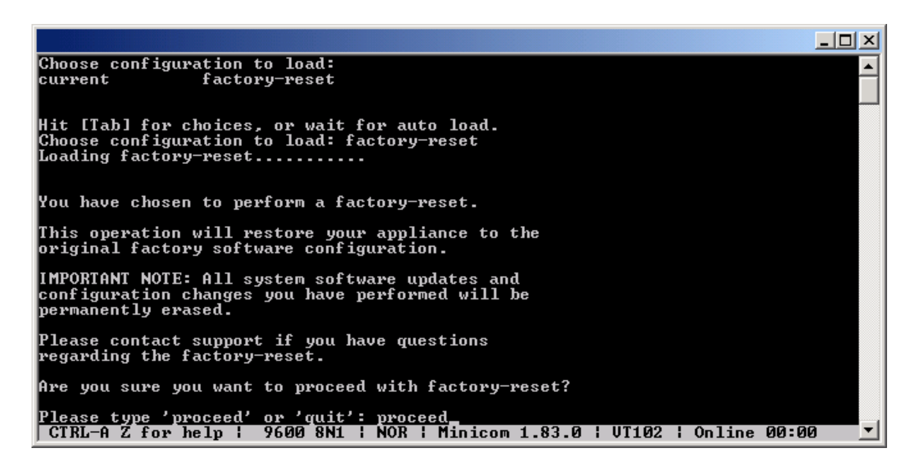


Abbildung 181: IVE Serielle Konsole
Hier wurde das Zurücksetzen auf die Werkseinstellungen ausgewählt.

Das System beginnt mit dem Zurücksetzen des Geräts auf die Originaleinstellungen und gibt dabei mehrere Bildschirme mit Daten aus. Nach einigen Minuten werden Sie aufgefordert, für die Auswahl von Kon-figurationsoptionen die **Tab-Taste** zu drücken.

```
LI

Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: _
```

Abbildung 182: IVE Serielle Konsole
Nach dem Zurücksetzen auf die Werkseinstellungen.

7. Wenn Sie zum Drücken der **Tab-Taste** aufgefordert werden, gibt es folgende Möglichkeiten:
   - Warten Sie den automatischen Start der Standardoption ab (`current`), oder
   - drücken Sie die **Tab-Taste**, geben Sie `current` ein, und drücken Sie dann die **Eingabetaste**.

   Sie werden dann aufgefordert, die ursprünglichen Konfigurationseinstellungen des Geräts einzugeben. Detaillierte Informationen zur Vorgehensweise können Sie dem Installations-handbuch entnehmen, das dem Gerät beiliegt. Dieses Handbuch steht auch auf der Juniper Networks-Supportsite im PDF-Format zur Verfügung.

   Nach dem Abschluss des Initialisierungsvorgangs können Sie auf das neueste Serverpaket aktualisieren und die gespeicherten System- und Benutzerkonfigurationsdateien importieren, um zum letzten funktionstüchtigen Zustand des Geräts zurückzukehren.

☑ Durchführen gängiger Wiederherstellungsvorgänge

Wenn Sie den Administratorbenutzernamen und/oder das Administratorkennwort für das IVE vergessen, sich aufgrund von Konfigurationsfehlern selbst vom Gerät ausgesperrt oder die IP-Adresse des IVE-Geräts geändert haben und nicht mehr auf das Gerät zugreifen können, können Sie die Geräteeinstellungen über die serielle Konsole ändern. Folgen Sie den Anweisungen unter „Herstellen einer Verbindung mit der seriellen Konsole des IVE“ auf Seite 567, und wählen Sie dann den gewünschten Konfigurationsvorgang aus.

- **Network Settings and Tools**

  Hiermit können Sie die Standardnetzwerkeinstellungen ändern, eine Routingtabelle ausgeben, den ARP-Cache ausgeben oder leeren, einen Ping-Befehl auf einen anderen Server ausführen, die Route zu einem anderen Server verfolgen, statische Routen entfernen und einen ARP-Eintrag hinzufügen.

- **Create admin username and password**

  Hiermit können Sie ein neues Super-Administratorkonto anlegen.

- **Display log**

  Hiermit können Sie die Systemkonfiguration, Benutzerprotokolle oder Protokolle des Administratorzugriffs über die serielle Konsole anzeigen. Nach dem Anzeigen der Protokolle müssen Sie „q" eingeben, um wieder die Optionen der seriellen Konsole anzuzeigen.

- **Reboot/Shutdown/Restart this IVE**

  Hiermit können Sie das IVE neu starten, herunterfahren oder neu starten, ohne die Webkonsole zu verwenden.

- **Toggle password protection for the console**

  Hiermit können Sie die Konsole durch ein Kennwort sichern. Wenn Sie diese Option auf „on" setzen, ist der Zugriff nur Super-Administratoren gestattet.

- **Erstellen einer Super-Administratorsitzung**

  Hiermit können Sie eine Wiederherstellungssitzung auf der Webkonsole erstellen, auch wenn der Administratorzugriff auf das IVE gesperrt ist. Wenn Sie diese Option aktivieren, generiert das IVE einen temporären Token, der drei Minuten gültig ist. Geben Sie den folgenden URL in ein Browserfenster ein: `https://<ive-host>/dana-na/auth/recover.cgi`. Geben Sie dann bei der entsprechenden Aufforderung den temporären Token ein, um sich an der Webkonsole anzumelden.

  Wichtig: Wenn Sie diese Option auswählen, sperrt das IVE alle weiteren Administratoren. Diese können sich dann nicht bei der Webkonsole anmelden, bis Sie sich am angegebenen URL angemeldet und die Sitzung mit ihrem Token gestartet haben. Das IVE sperrt weitere Anmeldeversuche, sodass Sie möglicherweise aufgetretene Konfigurationsprobleme beheben können, ohne dadurch in einer anderen Sitzung Störungen zu verursachen.

- **Replace Administrator Card Set (nur Access Series FIPS)**

  Hiermit können Sie weitere Administratorkarten für eine Security World erstellen. Weitere Informationen finden Sie im folgenden Abschnitt.

Hinweis: Wenn Sie ein Access Series FIPS-System ausführen und im Kryptographiemodul den Löschschalter gedrückt haben, stellen Sie den Modusschalter des Kryptographiemoduls auf **O** (Operationsmodus), und starten Sie das System neu. Zum Wiederherstellen benötigen Sie keinen Zugriff auf die serielle Konsole.

☑ Erstellen weiterer Administratorkarten (nur Access Series FIPS)

Um für eine Security World zusätzliche Administratorkarten erstellen zu können, müssen Sie über Folgendes verfügen:

- Ein Kryptographiemodul, das zur Security World gehört
- Einen Smartcardleser
- Eine Administratorkarte, die mit der Security World vorinitialisiert ist
- Eine oder mehrere unformatierte Smartcards oder Administratorkarten mit Daten, die Sie gefahrlos überschreiben können

---

Hinweis: Wenn Sie zusätzliche Smartcards benötigen, wenden Sie sich an Ihren IVE-Händler.

So erstellen Sie weitere Administratorkarten für eine Security World:

1. Schließen Sie das Kabel des Smartcardlesers am Lesegerätport eines Kryptographiemoduls an, das zur Security World gehört. Der Port befindet sich an der Frontplatte des IVE-Geräts.
2. Legen Sie eine vorinitialisierte Administratorkarte für die Security World mit den Kontakten nach oben in den Smartcardleser ein.
3. Stellen Sie den Modusschalter des Kryptographiemoduls auf **O** (Operationsmodus), sofern dieser sich nicht bereits in dieser Position befindet.
4. Stellen Sie eine Verbindung mit der seriellen Konsole her (Seite 567).
5. Wählen Sie in der Liste der Konfigurationsaufgaben den Eintrag **Replace Administrator Card Set**.
6. Geben Sie das Kennwort für die Security World ein.
7. Legen Sie nach der entsprechenden Aufforderung eine unformatierte Smartcard oder eine Administratorkarte, deren Daten Sie gefahrlos überschreiben können, mit den Kontakten nach oben in den Smartcardleser ein.
8. Geben Sie die angeforderten zusätzlichen Initialisierung-informationen ein.
9. Wiederholen Sie Schritt 7 für alle weiteren Karten, die Sie erstellen möchten.
10. Verwahren Sie mindestens eine der Administratorkarten an einem sicheren Ort.

☑ Erstellen einer neuen Security World (nur Access Series FIPS)

Sie können ein Access Series FIPS-Gerät erst verwenden, wenn Sie für dieses eine Security World erstellt haben. In manchen Fällen müssen Sie jedoch eine Security World mit einer neuen überschreiben. Wenn Sie z. B. eine Administratorkarte verlieren, sollten Sie eine völlig neue Security World erstellen, um zu verhindern, dass eine nicht vertrauenswürdige Person die Karte findet und auf Ihre Security World zugreifen kann. Auch wenn Sie das Kennwort für die ursprüngliche Security World vergessen haben, müssen Sie eine neue Security World erstellen.

Um eine neue Security World erstellen zu können, müssen Sie über Folgendes verfügen:

- Die Kryptographiemodule, die zur Security World gehören
- Einen Smartcardleser
- Eine oder mehrere unformatierte Smartcards oder Administratorkarten mit Daten, die Sie gefahrlos überschreiben können

---

Wichtig: Die alten Administratorkarten können für die neue Security World nur verwendet werden, wenn Sie sie mit den Daten der neuen Security World neu formatieren. Beachten Sie, dass der Prozess abgeschlossen werden muss, sobald der Schalter auf I gestellt und mit der Initialisierung begonnen wurde. Andernfalls wird die Security World nur teilweise initialisiert und ist somit nicht verwendungsfähig.

Informationen zum Überschreiben einer Security World mit einer vorhandenen Security World finden Sie unter „Wiederherstellen einer archivierten Security World (nur Access Series FIPS)“ auf Seite 576.

So erstellen Sie eine neue Security World für ein eigenständiges IVE:

1. Schließen Sie das Kabel des Smartcardlesers an den Lesegerätport des Kryptographiemoduls an, der sich an der Frontplatte des IVE-Geräts befindet.
2. Legen Sie eine unformatierte Smartcard oder eine Administratorkarte mit Daten, die Sie gefahrlos überschreiben können, mit den Kontakten nach oben in den Smartcardleser ein.
3. Stellen Sie den Modusschalter des Kryptographiemoduls auf I (Initialisierungsmodus).
4. Greifen Sie auf die serielle Konsole des IVE zu, und starten Sie das IVE (Seite 567) neu.
5. Geben Sie die angeforderten Initialisierungsinformationen ein.

6. Stellen Sie den Modusschalter des Kryptographiemoduls auf O (Operationsmodus) zurück, wenn Sie dazu aufgefordert werden.
7. Erstellen Sie ein neues Serverzertifikat, für das der neue private Schlüssel der Security World verwendet wird (Seite 187).

So erstellen Sie eine neue Security World in einer Clusterumgebung:

1. Melden Sie sich an der Webkonsole eines Clusterknotens an, den Sie mit einer neuen Security World neu formatieren möchten. Um auf die Webkonsole eines Knotens zuzugreifen, geben Sie in einem Browser seine interne IP-Adresse und „/admin" ein. Beispiel: https://x.x.x.x/admin
2. Aktivieren Sie auf der Registerkarte **System > Clustering > Status** in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens, und klicken Sie dann auf **Disable**.
3. Initialisieren Sie das Clustermitglied mit einer Security World. Gehen Sie folgendermaßen vor:
   - Wenn dies der erste Knoten im Cluster ist, erstellen Sie eine neue Security World (Seite 575).
   - Wenn dies ein nachfolgender Knoten im Cluster ist, initialisieren Sie das Gerät mit der vorhandenen Security World des Clusters (Seite 577).
4. Kehren Sie zur Registerkarte **System > Clustering > Status** des Knotens zurück, aktivieren Sie in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens, und klicken Sie dann auf **Enable**.
5. Führen Sie diese Schritte für jeden Knoten im Cluster durch.

☑ Wiederherstellen einer archivierten Security World (nur Access Series FIPS)

In seltenen Fällen müssen Sie das System mithilfe einer archivierten Security World wiederherstellen. Die archivierte Security World kann eine ältere Version als die im System vorhandene Security World sein oder mit dieser übereinstimmen. Um das System wiederherzustellen, müssen Sie auf die Systemkonfigurationsdatei (in der Standardeinstellung `system.cfg`) zugreifen können, die die archivierte Security World und das entsprechende Zertifikat enthält.

Wenn Sie ein Security World mit einer anderen Security World überschreiben, müssen Sie außerdem über Folgendes verfügen:

- Alle Kryptographiemodule, die zur Security World gehören
- Einen Smartcardleser

- Eine Administratorkarte, die mit der Security World und dem Administratorkennwort vorinitialisiert ist, die Sie importieren möchten

So importieren Sie eine vorhandene Security World in ein eigenständiges IVE:

1. Importieren Sie die Systemkonfigurationsdatei, die die archivierte Security World und das entsprechende Zertifikat enthält, in das IVE(Seite 530), und initialisieren Sie ggf. die Security World. Enthält die Konfigurationsdatei eine archivierte Version von:
   - Der Security World, die auf dem Computer bereits vorhanden war, ist keine weitere Konfiguration erforderlich.
   - Einer anderen Security World als der, die auf dem Computer bereits vorhanden war, müssen Sie die neue Security World initialisieren.

   Wichtig: Wenn Sie eine Konfigurationsdatei importieren, die eine andere Security World enthält, können Sie Ihre vorhandenen Administratorkarten erst für die importierte Security World verwenden, wenn Sie sie mit den Daten der neuen Security World neu formatiert haben. Beachten Sie, dass der Prozess abgeschlossen werden muss, sobald der Schalter auf I gestellt und mit der Initialisierung begonnen wurde. Andernfalls wird die Security World nur teilweise initialisiert und ist somit nicht verwendungsfähig.

   ---

2. Schließen Sie das Kabel des Smartcardlesers an den Lesegerätport des Kryptographiemoduls an, der sich an der Frontplatte des IVE-Geräts befindet.
3. Legen Sie eine Administratorkarte, die mit der importierten Security World vorinitialisiert wurde, mit den Kontakten nach oben in den Smartcardleser ein.
4. Stellen Sie den Modusschalter des Kryptographiemoduls auf I (Initialisierungsmodus).
5. Greifen Sie auf die serielle Konsole des IVE zu, und starten Sie das IVE (Seite 567) neu.
6. Geben Sie die angeforderten Initialisierungsinformationen ein.
7. Stellen Sie den Modusschalter des Kryptographiemoduls auf O (Operationsmodus) zurück, wenn Sie dazu aufgefordert werden.

So importieren Sie eine vorhandene Security World in einen Cluster:

1. Melden Sie sich an der Webkonsole eines Clusterknotens an, den Sie mit einer neuen Security World neu formatieren möchten. Um auf die Webkonsole eines Knotens zuzugreifen, geben Sie in einem Browser seine interne IP-Adresse und „/admin“ ein. Beispiel: https://x.x.x.x/admin

2. Aktivieren Sie auf der Registerkarte **System > Clustering > Status** in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens, und klicken Sie dann auf **Disable**.
3. Importieren Sie eine archivierte Security World in das Clustermitglied, wie im vorigen Abschnitt beschrieben.
4. Nach Abschluss des Installationsvorgangs kehren Sie zur Registerkarte **System > Clustering > Status** des Knotens zurück, aktivieren in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens und klicken dann auf **Enable**.
5. Führen Sie diese Schritte für jeden Knoten im Cluster durch.

Anhang B.

Authentifizierung und Autorisierung – Flussdiagramm

In diesem Flussdiagramm werden die Transaktionen zwischen Benutzer und IVE sowie zwischen IVE und Authentifizierungsbereich dargestellt. Das Flussdiagramm beginnt an dem Punkt, an dem ein Benutzer in der IVE-Anmeldungsseite einen URL eingibt und endet damit, dass der Benutzer die Benutzersitzung eigenständig beendet.

USER

IVE

Auth Server

User enters IVE URL in a browser

Examples:
https://employees.yourcompany.com/marketing
https://employees.yourcompany.com/admins
https://partner1.yourcompany.com

IVE evaluates sign-in policies

Starts with Administrator URLs and continues to User URLs until it matches the entered hostname. Upon match, displays the sign-in page for the URL and a list of authentication realms (if >1 realm exists and if the IVE is configured to do so).

User submits credentials

Enters username and password. If >1 authentication realm exists, enters realm or chooses realm from list.

IVE evaluates realm authentication policy for sign-in requirements

Users belonging to this realm may be restricted by:

- Source IP
- Browser type
- Client-side Certificate
- Password length
- Host Checker
- Cache Cleaner

Realm authentication policy check passed?

NO

User denied access to IVE

YES

IVE forwards user credentials to realm authentication server

Abbildung 183: **Schritt 1 von 3: IVE authentifiziert Benutzer**

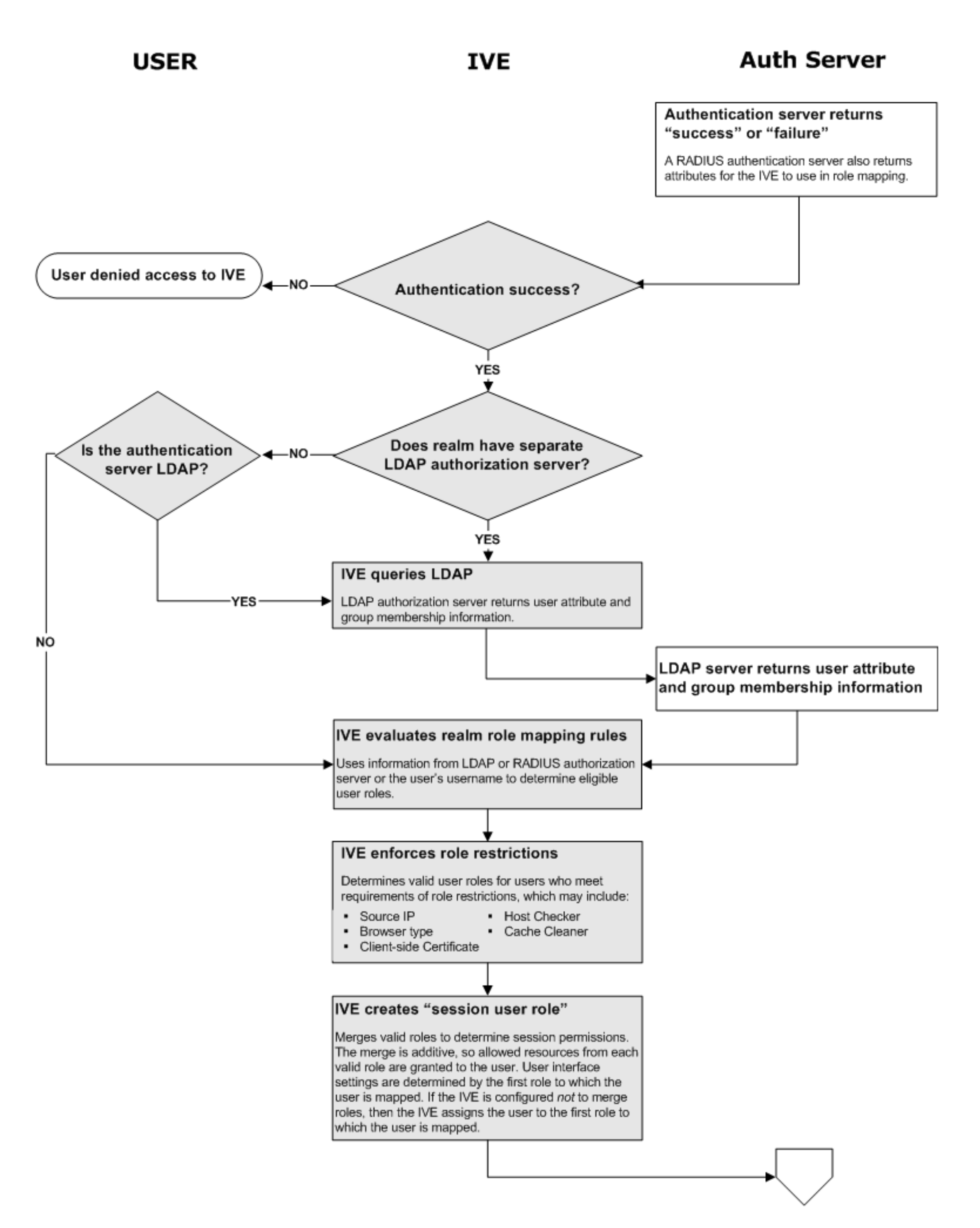


Abbildung 184: **Schritt 2 von 3: IVE ordnet den Benutzer zu einer oder mehreren Rollen zu**

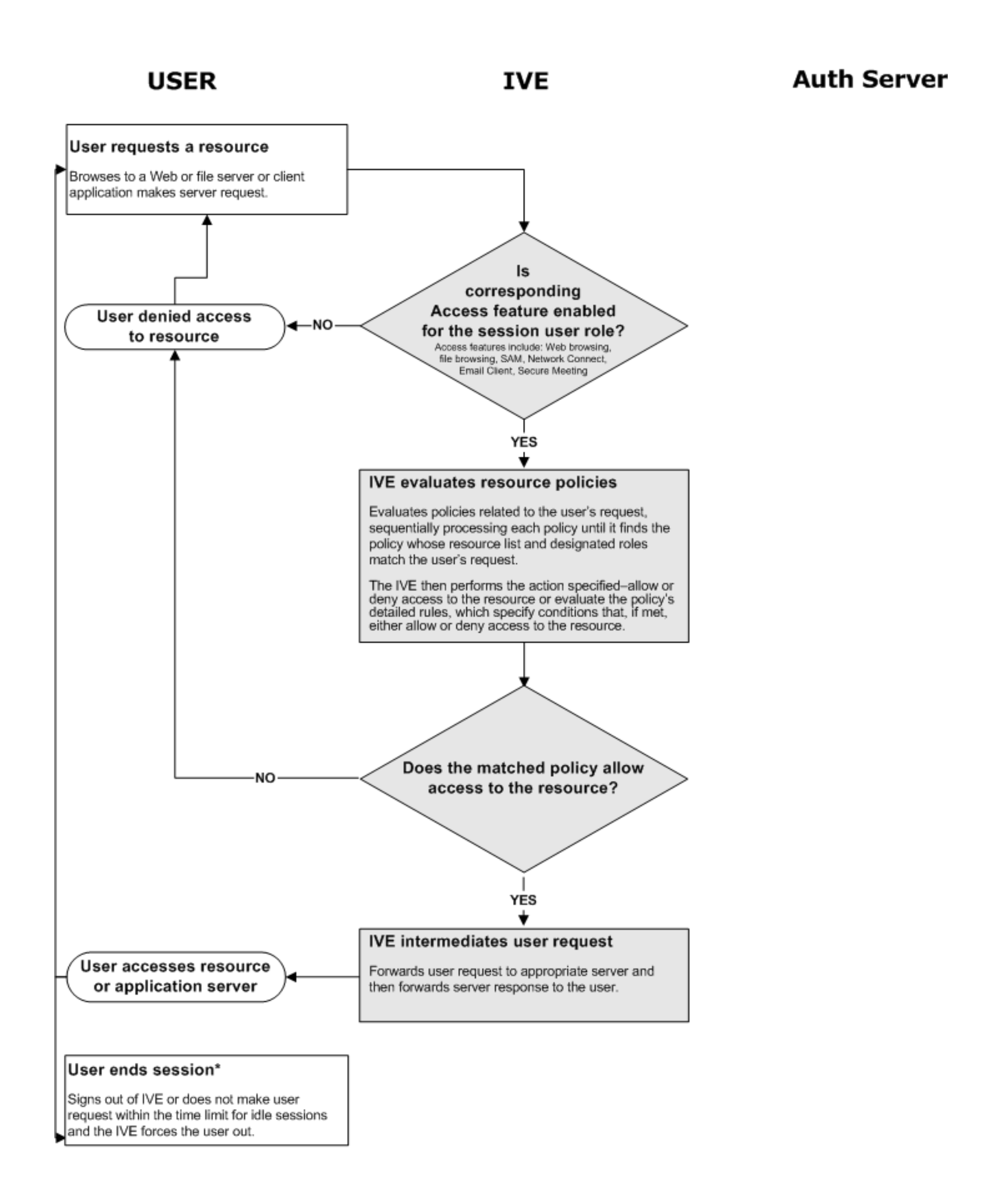


Abbildung 185: Schritt 3 von 3: IVE wertet die Ressourcenrichtlinien entsprechend der Benutzeranforderung aus

Anhang C.
Konfigurieren der Zugriffsverwaltungsoptionen

Das IVE ermöglicht Ihnen die Sicherung Ihrer Unternehmensressourcen auf drei Ebenen:

- **Bereich**

  Auf der Bereichsebene konfigurieren Sie die Anforderungen für die Zugriffsverwaltung in der Authentifizierungsrichtlinie.

- **Rolle**

  Auf der Rollenebene konfigurieren Sie die Anforderungen für die Zugriffsverwaltung entweder in den Rollenzuordnungsregeln der Authentifizierungsrichtlinie oder über die Einschränkungsoptionen für die Rolle.

- **Ressourcenrichtlinie**

  Auf der Ebene der Ressourcenrichtlinie konfigurieren Sie die Anforderungen für die Zugriffsverwaltung, indem Sie Bedingungen für Rollen schreiben.

Konfigurationsanweisungen für Optionen der Zugriffsverwaltung finden Sie unter:

Übersichtsinformationen finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 25.

Quell-IP-Einschränkungen

Mit einer Quell-IP-Einschränkung kann gesteuert werden, von welcher IP-Adresse aus Benutzer auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden können.

☑ Angeben von Quell-IP-Einschränkungen

So geben Sie Quell-IP-Einschränkungen auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP

- **Rollenebene**

  Navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Source IP
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Source IP

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Users can sign in from any IP address** – Hiermit können sich Benutzer von einer beliebigen IP-Adresse aus beim IVE anmelden, um die Anforderungen für die Zugriffsverwaltung zu erfüllen.
- **Users can only sign in from the following IP addresses** – Schränkt die Anzahl der IP-Adressen ein, von denen aus sich Benutzer anmelden können, um die Anforderungen für die Zugriffsverwaltung zu erfüllen. Wenn Sie diese Option auswählen, müssen Sie mindestens eine IP-Adresse angeben, da sonst keine Quell-IP-Einschränkung angewendet werden kann.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Browsereinschränkungen

Mit einer Browsereinschränkung kann gesteuert werden, von welchen Webbrowsern aus Benutzer auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden können. Wenn ein Benutzer versucht, sich im IVE über einen nicht unterstützten Browser anzumelden, schlägt der Anmeldeversuch fehl, und es wird in einer Meldung angezeigt, dass ein nicht unterstützter Browser verwendet wird. Mit dieser Funktion können Sie auch sicherstellen, dass sich Benutzer im IVE über Browser anmelden, die mit Firmenanwendungen kompatibel oder von Firmensicherheitsrichtlinien zugelassen sind.

Hinweis: Das Feature zur Browsereinschränkung dient nicht als strikte Zugriffssteuerung, da die Zeichenfolgen für Benutzer-Agenten des Browsers von einem technischen Benutzer geändert werden können. Es dient als beratende Zugriffssteuerung für normale Nutzungsszenarien.

☑ Angeben von Browsereinschränkungen

So geben Sie Browsereinschränkungen auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser

- **Rollenebene**

  Navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Browser
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Browser

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Allow all users matching any user-agent string sent by the browser** – Ermöglicht Benutzern den Zugriff auf das IVE oder auf Ressourcen mit einem beliebigen unterstützten Webbrowser.
- **Only allow users matching based on the user-agent string sent by the browser** – Ermöglicht Ihnen die Definition von Regeln für die Browserzugriffssteuerung. So erstellen Sie eine Regel:

  1. Geben Sie für **User-agent string pattern** eine Zeichenfolge in folgendem Format ein:

     ```
     *<browser_zeichenfolge>*
     ```

     wobei Start (*) ein optionales Zeichen ist, das für ein beliebiges Zeichen steht, und `<browser_zeichenfolge>` ein Muster darstellt (Groß- und Kleinschreibung wird berücksichtigt), das mit einer Teilzeichenfolge im „User-Agent"-Header übereinstimmen muss, der vom Browser gesendet wurde.

  2. Wählen Sie eine der folgenden Optionen aus:
     Allow, um Benutzern die Verwendung eines Browsers mit einem „User-Agent"-Header zu ermöglichen, der die Teilzeichenfolge `<browser_zeichenfolge>` enthält, oder
     Deny, um Benutzern die Verwendung eines Browsers mit einem „User-Agent"-Header zu verweigern, der die Teilzeichenfolge `<browser_zeichenfolge>` enthält.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Hinweis

- Regeln werden der Reihenfolge nach angewendet, d. h., die erste übereinstimmende Regel wird angewendet.
- Bei Literalzeichen in Regeln wird die Groß- und Kleinschreibung beachtet, Leerzeichen sind dabei zulässig.

Beispiele

- Die Zeichenfolge `*Netscape*` findet für alle für Benutzer-Agent-Zeichenfolgen eine Übereinstimmung, die die Teilzeichenfolge `Netscape` enthält.
- Der folgende Regelsatz ermöglicht Ressourcenzugriff nur dann, wenn Benutzer über Internet Explorer 5.5x oder Internet Explorer 6.x angemeldet sind. In diesem Beispiel werden einige wichtige andere Browser als Internet Explorer berücksichtigt, die die Teilzeichenfolge „MSIE" im „User-Agent"-Header senden:

  `*Opera*`**Deny**

  `*AOL*`**Deny**

  `*MSIE 5.5*`**Allow**

  `*MSIE 6.*`**Allow**

  `*` **Deny**

Zertifikateinschränkungen

Legen Sie anhand einer Zertifikateinschränkung fest, dass Clientcomputer über ein gültiges clientseitiges Zertifikat verfügen müssen, um auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden zu können. Wenn Sie dieses Feature verwenden, stellen Sie sicher, dass Sie ein Zertifikat einer Zertifizierungsstelle importieren, um das clientseitige Zertifikat zu überprüfen (wie unter „Registerkarte „Certificates > CA Certificates"" auf Seite 190 erläutert). Um die Sicherheit dieses Features zu optimieren, sollten die Clienteinstellungen eines Benutzers so festgelegt werden, dass der Benutzer bei jeder Anmeldung ein Kennwort eingeben muss. In der Standardeinstellung wird bei einigen Browserversionen das Zertifikatkennwort gespeichert, d. h. der Benutzer wird nach Installation des Zertifikats nicht zur Eingabe dieser zusätzlichen Anmeldeinformationen aufgefordert.

☑ Angeben clientseitiger Zertifikateinschränkungen

Die Stammzertifizierungsstelle, die zur Überprüfung der Clientzertifikate verwendet werden soll, wird folgendermaßen angegeben: System > Configuration > Certificates > CA Certificates

So geben Sie Zertifikateinschränkungen auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

- **Rollenebene**

  Navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Certificate
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Certificate

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Allow all users (no client-side certificate required)** – Clients von Benutzern müssen nicht über ein clientseitiges Zertifikat verfügen.
- **Only allow users with a client-side certificate signed by Certification Authority to sign in** – Legt fest, dass der Client eines Benutzers über ein clientseitiges Zertifikat verfügen muss, um die Anforderungen für die Zugriffsverwaltung zu erfüllen. Um den Zugriff noch weiter einzuschränken, können Sie eindeutige Attribut-Wert-Paare für das Zertifikat festlegen. Beachten Sie, dass das Zertifikat des Benutzers alle von Ihnen definierten Attribute enthält.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Hinweis

- Alle X.509-DN-Attribute (Distinguished Name) werden unterstützt (z. B. C, CN, L, O, OU).
- Bei den Attribut- und Wertefeldern wird die Groß- und Kleinschreibung nicht beachtet.
- Definieren Sie für jedes Attribut nur einen Wert. Wenn Sie mehrere Werte angeben, kann das clientseitige Zertifikat möglicherweise nicht ordnungsgemäß anhand des Zertifikats der Zertifizierungsstelle authentifiziert werden.

Kennworteinschränkung

Verwenden Sie eine Kennworteinschränkung, um eine minimale erforderliche Kennwortlänge für den Bereich festzulegen.

☑ Angeben einer Kennwortlängeneinschränkung

So geben Sie eine Kennworteinschränkung auf der Bereichsebene ein:

Navigieren Sie zu:

- Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password
- Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Allow all users (passwords of any length)** – Für Benutzer, die sich beim IVE anmelden, wird keine Kennwortlängeneinschränkung angewendet.
- **Only allow users that have passwords of a minimum length** – Bei dieser Option muss das einzugebende Kennwort eine festgelegte Anzahl von Zeichen lang sein.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Hinweis

Für das IVE müssen die auf der Anmeldeseite eingegebenen Benutzerkennwörter standardmäßig mindestens vier Zeichen lang sein. Für den zur Überprüfung der Anmeldeinformationen eines Benutzers verwendeten Authentifizierungsserver ist unter Umständen eine andere Mindestlänge erforderlich. Für die lokale Authentifizierungsdatenbank von IVE müssen die Benutzerkennwörter beispielsweise mindestens sechs Zeichen lang sein.

Hostprüfungseinstellungen

Legen Sie anhand einer Hostprüfungseinschränkung fest, dass Clientcomputer die angegebenen Hostprüfungsrichtlinien erfüllen müssen, um auf eine IVE-Anmeldeseite oder eine Ressourcenrichtlinie zugreifen oder einer Rolle zugeordnet werden zu können.

☑ Angeben von Hostprüfungseinschränkungen

Systemweite Richtlinien für die Hostprüfung werden folgendermaßen angegeben: System > Configuration > Security > Hostprüfung

So geben Sie Einschränkungen für Hostprüfung auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Hostprüfung
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Hostprüfung

- **Rollenebene**

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Hostprüfung
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Hostprüfung

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wenn Sie eine Hostprüfung-Anforderung der ***Bereichsebene*** konfigurieren, wählen Sie eine der folgenden Optionen aus:

- **Allow all users** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn die Hostprüfung nicht installiert ist.

- **Allow all users & install Host Checker** – Legt fest, dass das IVE die Hostprüfung auf den Clientcomputer herunterladen muss. Wenn Sie diese Option für die Authentifizierungsrichtlinie eines Bereichs auswählen, lädt das IVE die Hostprüfung auf den Clientcomputer herunter, nachdem der Benutzer authentifiziert, aber bevor er Rollen im System zugeordnet wurde.
- **Allow only users whose workstations meet the requirements specified by the following** [Richtlinien] – Der Benutzer erfült die Zugriffsvoraussetzungen nur, wenn die Hostprüfung die angegebene Richtlinie für die Hostprüfung ausführt. Wenn Sie diese Option für die Authentifizierungsrichtlinie eines Bereichs auswählen, lädt das IVE die Hostprüfung auf den Clientcomputer herunter, bevor der Benutzer auf die IVE-Anmeldeseite zugreifen kann.

Wenn Sie eine Hostprüfung-Anforderung auf ***Rollenebene*** konfigurieren, wählen Sie eine der folgenden Optionen aus:

- **Allow all users** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn die Hostprüfung nicht installiert ist.
- **Allow only users whose workstations meet the requirements specified by the following** [Richtlinien] – Der Benutzer erfült die Zugriffsvoraussetzungen nur, wenn die Hostprüfung die angegebene Richtlinie für die Hostprüfung ausführt.

Sie können auch einen benutzerdefinierten Ausdruck für die Rollenzuordnungsregel schreiben, um den Status von Hostprüfung anhand der Variable `hostCheckerPolicy` auszuwerten. Zum Erstellen von Hostprüfung-Einschränkungen auf der ***Ressourcenrichtlinienebene*** müssen Sie einen benutzerdefinierten Ausdruck in einer detaillierten Regel erstellen.

Einschränkungen für Cachebereinigung

Legen Sie anhand einer Einschränkung für Cachebereinigung fest, dass Clientcomputer die angegebenen Richtlinien für Cachebereinigung erfüllem müssen, um auf eine IVE-Anmeldeseite bzw. eine Ressourcenrichtlinie zugreifen oder einer Rolle zugeordnet werden können.

☑ Angeben von Einschränkungen für Cachebereinigung

Systemweite Richtlinien für die Cachebereinigung werden folgendermaßen angegeben: System > Configuration > Security > Cachebereinigung

So geben Sie Einschränkungen für Cachebereinigung auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Cachebereinigung
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Cachebereinigung

- **Rollenebene**
  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Cachebereinigung
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Cachebereinigung

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wenn Sie eine Cachebereinigung-Anforderung der ***Bereichsebene*** konfigurieren, wählen Sie eine der folgenden Optionen aus:

- **Disable Cachebereinigung** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn Cachebereinigung nicht installiert ist oder ausgeführt wird.
- **Just load Cache CleanerCachebereinigung** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn Cachebereinigung nicht ausgeführt wird, diese ist jedoch für eine spätere Verwendung verfügbar. Wenn Sie diese Option für die Authentifizierungsrichtlinie eines Bereichs auswählen, wird Cachebereinigung von IVE auf den Clientcomputer heruntergeladen, nachdem der Benutzer authentifiziert, aber bevor er Rollen im System zugeordnet wurde.
- **Load and enforce Cache** – Der Benutzer erfüllt die Zugriffsanforderungen nur, wenn Cachebereinigung von IVE heruntergeladen und ausgeführt wird. Wenn Sie diese Option für die Authentifizierungsrichtlinie eines Bereichs auswählen, wird Cachebereinigung von IVE auf den Clientcomputer heruntergeladen, bevor der Benutzer auf die IVE-Anmeldeseite zugreifen kann.

Aktivieren Sie zum Konfigurieren einer Anforderung für Cachebereinigung auf ***Rollenebene*** die folgende Option:

- **Enable Cachebereinigung** – Der Benutzer erfüllt die Zugriffsanforderungen nur, wenn Cachebereinigung ausgeführt wird.

Sie können auch einen benutzerdefinierten Ausdruck für die Rollenzuordnungsregel schreiben, um den Status von Cachebereinigung anhand der Variable `cacheCleaner` auszuwerten. Zum Erstellen von Cachebereinigung-Einschränkungen auf der ***Ressourcen-richtlinienebene*** müssen Sie einen benutzerdefinierten Ausdruck in einer detaillierten Regel erstellen.

Anhang D.

Schreiben benutzerdefinierter Ausdrücke

Mit dem IVE können Sie benutzerdefinierte Ausdrücke schreiben, die in Rollenzuordnungsregeln, Ressourcenrichtlinien und Protokollfilterabfragen ausgewertet werden. Ein ***benutzerdefinierter Ausdruck*** ist eine Kombination von Variablen, die das IVE als boolesches Objekt als „true" (wahr), „false" (falsch) oder error (Fehler) auswertet. Mithilfe von benutzerdefinierten Ausdrücken können Sie komplexe Bedingungen für Richtlinienauswertung und Protokollabfragen erstellen, die die Ressourcenzugriffskontrolle verbessern und erleichtern. Sie können benutzerdefinierte Ausdrücke in den folgenden Formaten schreiben:

Syntax für benutzerdefinierte Ausdrücke

```
variable comparisonOperator variable
variable comparisonOperator simpleValue
variable comparisonOperator (simpleValue)
variable comparisonOperator (ORValues)
variable comparisonOperator (ANDValues)
variable comparisonOperator (time TO time)
variable comparisonOperator (day TO day)
isEmpty (variable)
isUnknown (variable)
(customExpr)
NOT customExpr
! customExpr
customExpr OR customExpr
customExpr || customExpr
customExpr AND customExpr
customExpr && customExpr
```

Dabei ist:

`variable` ist eine Systemvariable. Ein Variablenname ist eine durch Punkte getrennte Zeichenfolge. Jede Komponente darf Zeichen aus dem Bereich [a-z A-Z 0-9_] enthalten, darf jedoch nicht mit einer Ziffer [0-9] starten. Bei Variablennamen wird die Groß- und Kleinschreibung nicht berücksichtigt. Systemvariablen, die in Rollenzuordnungsregeln und -ressourcen verwendet werden können, finden Sie unter „Systemvariablen und Beispiele“ auf Seite 601[1].

Maskierte Syntax für Variablen

Das IVE unterstützt eine maskierte Syntax für Variablen benutzerdefinierter Ausdrücke, die die Verwendung aller Zeichen außer '.' (Punkt) in Benutzerattributnamen ermöglicht. Um in Attributnamen Escape-Zeichen zu verwenden, maskieren Sie Teile des Variablennamens oder den gesamten Namen mit { } (geschweifte Klammern). Beispielsweise entsprechen sich folgende Ausdrücke:

```
userAttr.{Login-Name} = 'xyz'
userAttr.Login{-}Name = 'xyz'
{userAttr.Login-Name} = 'xyz'
userA{ttr.L}{ogin-}Name = 'xyz'
```

Innerhalb von Maskierungen werden die folgenden Escape-Zeichen unterstützt:

`\\` steht für `\` (umgekehrter Schrägstrich)

`\{` steht für `{` (linke geschweifte Klammer)

`\}` steht für `}` (rechte geschweifte Klammer)

`\hh` steht für einen hexadezimalen Wert, wobei hh zwei Zeichen von [0-9A-Fa-f] darstellt

Beispiele:

```
userAttr.{Tree Frog} = 'kermit'
userAttr.{Tree\20Frog} = 'kermit'
```

Hinweise:
- Die Anzahl der Maskierungen, die in einem Variablennamen verwendet werden können, ist unbegrenzt.
- Sie können die maskierte Syntax nicht nur mit userAttr.*-Variablen, sondern mit allen Variablen verwenden.
- Maskierungen aus geschweiften Klammern müssen nur bei benutzerdefinierten Ausdrücken verwendet werden.

`comparisonOperator` kann folgende Werte annehmen:

=	gleich – Kann für Zeichenfolgen, Zahlen und DNs verwendet werden
!=	ungleich – Kann für Zeichenfolgen, Zahlen und DNs verwendet werden
<	kleiner als – Kann mit Zahlen verwendet werden
<=	kleiner oder gleich – Kann mit Zahlen verwendet werden
>	größer als – Kann für Zahlen verwendet werden
>=	größer oder gleich – Kann für Zahlen verwendet werden

`simpleValue` kann folgende Werte annehmen:

- Zeichenfolge – Zeichenfolge in Anführungszeichen, die Platzhalter enthalten kann
- IP-Adresse – a.b.c.d
- Subnetz – a.b.c.d/Subnetz Anzahl Bits oder a.b.c.d/Netmask
- Zahl – positive oder negative Ganzzahl
- Tag[2] – SUN MON TUE WED THU FRI SAT

Hinweise zu Zeichenfolgen:

- Eine Zeichenfolge kann alle Zeichen außer <nl> und <cr> enthalten.
- Bei Zeichenfolgenvergleichen wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Zeichenfolgen können in einfache oder doppelte Anführungszeichen gesetzt werden. Eine Zeichenfolge in Anführungsstrichen kann Platzhalter enthalten, d. h. Sternchen (*), Fragezeichen (?) und eckige Klammern ([ ]). Weitere Informationen finden Sie unter „Platzhalterabgleich“ auf Seite 599.
- Vergleiche vom Typ *variable comparisonOperator variable* werden ohne Platzhalterabgleich ausgewertet.
- Verwenden Sie einen umgekehrten Schrägstrich als Escape-Zeichen für die folgenden Zeichen:
  einfaches Anführungszeichen (') – \'
  doppeltes Anführungszeichen (") – \"
  umgekehrter Schrägstrich (\) – \\
  Hexadezimalzahl – \hh [0-9a-fA-F]

`time`[2] ist die Uhrzeit in einem der folgenden Formate:

SS:MM – 24-Stunden-Format
SS:MMam – 12-Stunden-Format
SS:MMpm – 12-Stunden-Format
S:MM – 24-Stunden-Format
S:MMam – 12-Stunden-Format
S:MMpm – 12-Stunden-Format

`ORValue` ist eine Zeichenfolge, die einen oder mehrere OR-Vergleiche enthält:

Variable comparisonOperator (Zahl AND Zahl...)

Variable comparisonOperator (Zeichenfolge AND Zeichenfolge...)

`ANDValue` ist eine Zeichenfolge, die einen oder mehrere AND-Vergleiche enthält:

Variable comparisonOperator (Zahl AND Zahl ...)

Variable comparisonOperator (Zeichenfolge AND Zeichenfolge...)

`isEmpty` ist eine Funktion, die eine einzelne Variable als Argument nimmt und einen booleschen Wert zurückgibt. isEmpty() ist „true“, wenn die Variable unbekannt ist, eine Länge von Null hat oder Zeichenfolgen der Länge Null bzw. leere Listen enthält.

Beispiel: isEmpty(userAttr.terminationDate)

`isUnknown` ist eine Funktion, die eine einzelne Variable als Argument nimmt und einen booleschen Wert zurückgibt. isUnknown() ist „true“, wenn die Variable nicht definiert ist. Benutzerattribute (userAttr.*-Variablen) sind unbekannt, wenn das Attribut nicht in LDAP definiert ist oder wenn der Attribut-Lookup fehlschlägt (wenn z. B. der LDAP-Server außer Betrieb ist).

Beispiel: isUnknown(userAttr.bonusProgram)

`NOT, !` ist der Vergleichsoperator für die logische Negation. Der negierte Ausdruck ergibt „true“, wenn der benutzerdefinierte Ausdruck „false“ ist und „false“, wenn der benutzerdefinierte Ausdruck „true“ ist[3].

`OR, ||` ist der logische Operator OR oder ||, die äquivalent sind[3].

`AND, &&` ist der logische Operator AND oder &&, die äquivalent sind[3].

`customExpr` ist ein in der Syntax für benutzerdefinierte Ausdrücke geschriebener Ausdruck (siehe oben)

1 Zum Schreiben eines benutzerdefinierten Ausdrucks in einem Protokollabfragefeld müssen Sie Systemprotokollvariablen verwenden.
2 Tag- und Zeitvergleiche werden in der Zeitzone des IVE ausgewertet. Berechnungen der Tagesbereiche (Tag **TO** Tag) beginnen mit dem ersten angegebenen Tag und werden schrittweise ausgeführt, bis der zweite angegebene Tag erreicht wird. In Berechnungen für Zeitbereiche (time **TO** time) muss der erste Wert zeitlich vor dem zweiten Wert liegen. Nur Zeitvariablen können mit Tages- und Zeitwerten verglichen werden. Zeitvariablen sind: `time.*` und `loginTime.*`
3 Die Operatoren NOT, AND und OR werden von der höchsten zur niedrigsten Priorität in folgender Rangfolge ausgewertet: NOT (von rechts), AND (von links), OR (von links)

Platzhalterabgleich

In einer Zeichenfolge, die in Anführungszeichen eingeschlossen ist, können Platzhalter verwendet werden. Folgende Platzhalter werden unterstützt:

- **Sternchen (*)**

  Ein Sternchen steht für eine beliebige Folge von null oder mehr Zeichen.

- **Fragezeichen (?)**

  Ein Fragezeichen steht für ein einzelnes Zeichen.

- **Eckige Klammern ([ ])**

  Eckige Klammern stehen für ein Zeichen aus einem Bereich möglicher Zeichen, der zwischen den Klammern angegeben wird. Zwei durch einen Bindestrich (-) getrennten Zeichen stehen für die beiden Zeichen und die lexikalisch dazwischen liegenden Zeichen. Beispiel: 'dept[0-9]' steht anstelle der Zeichenfolgen „dept0", „dept1" usw. bis einschließlich „dept9".

Die Escape-Zeichen für Platzhalter sind eckige Klammern. So ergibt der Ausdruck ' userAttr.x = "value[*]" ' beispielsweise „true", wenn das Attribut x genau gleich „value*" ist.

DN-Variablen

Sie können einen Distinguished Name (DN) mit einem anderen DN oder einer Zeichenfolge vergleichen, Platzhalter werden dabei jedoch ignoriert. Bei Vergleichen wird die Groß- und Kleinschreibung nicht berücksichtigt, Leerzeichen werden ignoriert, und die Reihenfolge der DN-Schlüssel wird berücksichtigt.

Wenn ein Ausdruck einen DN mit einer Zeichenfolge vergleicht, wird diese vor der Auswertung des Ausdrucks in einen DN konvertiert. Wenn die Zeichenfolge (aufgrund fehlerhafter Syntax) nicht konvertiert werden kann, schlägt der Vergleich fehl. DN-Variablen sind:

- userDN
- certDN
- certIssuerDN

Systemvariablen und Beispiele

Hinweis: Diese Liste enthält keine Variablen, die in einer Filterabfrage oder einem Exportformat für ein Systemprotokoll verwendet werden.

Variablen	Beschreibung	Beispiele
auth Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Name des Authentifizierungsservers, der einen Benutzer authentifiziert.	auth = ‘MyLDAPServer’
cacheCleaner Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Status der Cachebereinigung. Mögliche Werte: 1 - wenn sie ausgeführt wird 0 - wenn sie nicht ausgeführt wird	cacheCleanerStatus = 1 cacheCleanerStatus = 0

certAttr.<*cert-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • LDAP-Konfiguration • Felder für SSO-Parameter	Attribute eines clientseitigen Zertifikats. Beispiele für `certAttr`-Attribute: C - Country (engl. für Land) CN - Common Name (engl. für üblicher Name) description - Beschreibung emailAddress - E-Mail-Adresse GN - Given Name (engl. für Vorname) initials - Initialen L - Locality Name (engl. für Ortsname) O - Organization (engl. für Organisation) OU - Organizational Unit (engl. für Organisationseinheit) SN - Surname (engl. für Nachname) serialNumber- Serial Number (engl. für Seriennumer) ST - State/Province (Bundesland/Kanton) title - Titel UI - Unique Identifier (engl. für eindeutiger Bezeichner) Mithilfe dieser Variable können Sie überprüfen, ob der Client des Benutzers über ein clientseitiges Zertifikat mit den angegebenen Werten verfügt.	certAttr.OU = 'Retail Products Group'
CertAttr.altName.<*Alt-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • LDAP-Konfiguration • Felder für SSO-Parameter	Wert des alternativen Namens des Subjekts aus einem clientseitigen Zertifikat, wobei <*Alt-attr*> folgende Werte annehmen kann: .Email .directoryName .DNS .URI .ipAddress .registeredId	certAttr.altName.email = "joe@company.com" certAttr.altName.directoryName = "cn=joe, ou=company, o=com" certAttr.altName.ipAddress = 10.10.83.2

certAttr.SerialNumber Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • LDAP-Konfiguration • Felder für SSO-Parameter	Seriennummer eines Clientzertifikats. Beachten Sie, dass alle Zeichen außer [0-9 a-f A-F] aus einer Zeichenfolge vor dem Vergleich mit certAttr.SN entfernt werden. Platzhalter werden nicht unterstützt.	certAttr.SerialNumber = userAttr.certSerial certAttr.SerialNumber = "6f:05:45:ab"
certDN Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	DN des Clientzertifikat-Subjekts. Platzhalter sind nicht zulässig.	certDN = 'cn=John Harding,ou=eng,c=Company' certDN = userDN *(DN des Zertifikat-Subjekts wird mit dem DN des LDAP-Benutzers abgeglichen)* certDN = userAttr.x509SubjectName certDN = ('cn=John Harding,ou=eng,c=Company' or 'cn=Julia Yount,ou=eng,c=Company')
certDN.<*subject-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • LDAP-Konfiguration • Felder für SSO-Parameter	Beliebige Variable aus dem DN des Clientzertifikat-Subjekts, wobei *subject-attr* der Name des RDN-Schlüssels ist. Kann zum Testen verschiedener DN-Attribute in einem Standard-x.509-Zertifikat verwendet werden.	certDN.OU = 'company' certDN.E = 'joe@company.com' certDN.ST = 'CA'
certDNText Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Benutzer-DN eines Clientzertifikats. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	certDNText = 'cn=John Harding,ou=eng,c=Company'
certIssuerDN Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Subjekt-DN des Clientzertifikat-Ausstellers. Diese Variable verhält sich wie ein Standard-DN-Attribut (wie z. B. CertDN). Platzhalter sind nicht zulässig.	certIssuerDN = 'cn=John Harding,ou=eng,c=Company' certIssuerDN = userAttr.x509Issuer certIssuerDN = ('ou=eng,c=Company' or 'ou=operations,c=Company')

certIssuerDN.<*issuer-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Beliebige Variable aus dem Subjekt-DN des Clientzertifikat-Ausstellers, wobei *issuer-attr* der Name des RDN-Schlüssels ist.	certIssuerDN.OU = 'company' certIssuerDN.ST = 'CA'
certIssuerDNText Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Subjekt-DN des Clientzertifikat-Ausstellers. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	certIssuerDNText = 'cn=John Harding,ou=eng,c=Company'
group.<*group-name*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln **Wichtig:** Nur für Rollenzuordnung Rollenzuordnungsregeln ausgewerteten Attribute sind in den detaillierten Rollen (Bedingungen) in den Ressourcenrichtlinien verfügbar. Wir empfehlen die Verwendung der Gruppenvariable anstelle von group.<group-name>, das nur aus Gründen der Abwärtskompatibilität unterstützt wird.	Von der Bereichsauthentifizierung oder dem Verzeichnisserver bereitgestellte Gruppenmitgliedschaft von Benutzern. **Hinweis:** Leerzeichen werden nicht unterstützt, z. B.: group.sales managers	group.preferredPartner group.goldPartner or group.silverPartner group.employees and time.month = 9 ***Beispiele für Kombinationen:*** *Erlaubt alle Partner mit dem Status „Aktiv" von Montag bis Freitag, jedoch bevorzugte Partner von Montag bis Samstag:* ((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active' Hinweis: group.sales managers wird nicht unterstützt.

groups Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Von der Bereichsauthentifizierung oder dem Verzeichnisserver bereitgestellte Gruppenlisten.	groups=('sales managers')
hostCheckerPolicy Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Vom Client erfüllte Host Checker-Richtlinien.	hostCheckerPolicy = ('Norton' and 'Sygate') and cacheCleanerStatus = 1
loginTime Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Die Uhrzeit, zu der der Benutzer seine Anmeldeinformationen an das IVE sendet. Die Zeit basiert auf der IVE-Zeit. Hinweis: Bei Verwendung dieser Variable in einem SSO-Parameterfeld gibt die Variable die UNIX string time (Zeichenfolge, die die Uhrzeit enthält) zurück.	loginTime = (8:00am to 5:00pm) loginTime= (Mon to Fri)
loginTime.day Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Tag des Monats, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „day“ einen Wert von 1-31 annehmen kann. Die Zeit basiert auf der IVE-Zeit.	loginTime.day = 3

loginTime.dayOfWeek Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Wochentag, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet. „dayOfWeek“ kann im Bereich [0-6] liegen (0 = Sonntag).	loginTime.dayOfWeek != (0 OR 6) loginTime.dayOfWeek = (1 bis 5) loginTime.dayOfWeek = (Montag bis Freitag) loginTime.dayOfWeek = 5 loginTime.dayOfWeek = Freitag
loginTime.dayOfYear Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der numerische Tag des Jahres, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „dayOfYear“ auf [0-365] gesetzt werden kann.	loginTime.dayOfYear = 100
loginTime.month Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Monat, in dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „month“ auf [1-12] gesetzt werden kann (1 = Januar).	loginTime.month >= 4 AND loginTime.month <=9
loginTime.year Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Das Jahr, in dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „year“ auf [1900-2999] gesetzt werden kann.	loginTime.year = 2005
networkIf Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Die Netzwerkschnittstelle, an der eine Benutzerabfrage empfangen wird. Mögliche Werte: „internal“, „external“	sourceIp = 192.168.1.0/24 und networkIf = internal

Bereich Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Der Name des Authentifzierungsbereichs, an dem der Benutzer angemeldet ist.	Realm = ('GoldPartners' or 'SilverPartners') ***Hinweis:*** *Die Bedingung AND führt zu keinem Ergebnis, da sich ein Benutzer in einer Sitzung nur an einem einzigen Bereich anmelden kann.*
Rolle Verfügbar in: • Ressourcenrichtlinien-regeln • SSO	Liste aller Benutzerrollen für eine Sitzung. Wenn Sie in SSO alle Rollen an Back-End-Anwendungen senden möchten, verwenden Sie <role *sep* = ";"> – wobei *sep* die Zeichenfolge zum Trennen mehrerer Werte ist.	Role = ('sales' or 'engineering') Role = ('Sales' AND 'Support')
sourceIP Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Die IP-Adresse des Geräts, auf dem sich der Benutzer authentifiziert. Sie können die Netzmaske mit der Bitzahl oder im Netzmaskenformat angeben: '255.255.0.0'	sourceIP = 192.168.10.20 sourceIP = 192.168.1.0/24 und networkIf internal userAttr.dept = ('eng' or 'it') and sourceIP = 10.11.0.0/16 sourceIP = 192.168.10.0/24 *(Klasse C) ist identisch mit* sourceIP = 192.168.10.0/255.255.255.0

Zeit Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Die Uhrzeit, zu der die Rollenzuordnungsregel oder die Ressourcenrichtlinienregel ausgewertet wird. Die Uhrzeit kann im 12- oder 24-Stunden-Format angegeben werden.	time = (9:00am to 5:00pm) time = (09:00 to 17:00) time = (Mon to Fri) ***Beispiele für Kombinationen:*** *Erlaubt leitenden Angestellten und deren Assistenten den Zugriff von Montag bis Freitag:* userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri)
time.day Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Tag des Monats, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „day“ einen Wert von 1-31 annehmen kann. Die Zeit basiert auf der IVE-Zeit.	loginTime.day = 3
time.dayOfWeek Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Wochentag, an dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: Mon, Tue, Wed, Thu, Fri, Sat, Sun	time.dayOfweek = (Mon to Fri) time.dayOfWeek = (mon to fri) and time = (9:00am to 5:00pm) time.dayOfWeek = (sat to sun) and time = (8:00 to 23:00)
time.dayOfYear Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Tag im Jahr, an dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: 1-365.	time.dayOfYear = 100

time.month Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Monat, in dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: 1-12	time.month >= 9 and time.month <= 12 and time.year = 2004 group.employees and time.month = 9
time.year Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Das Jahr, in dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. „year“ kann auf [1900-2999] gesetzt werden	time.year = 2005
Benutzer Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	IVE-Benutzername. Wenn sich der Benutzer an einem Zertifikat-Authentifizierungsserver anmeldet, ist sein IVE-Benutzername derselbe wie CertDN.cn.	user = 'steve' and time = mon user = 'steve' user = 'steve*' user = ('steve' or '*jankowski')
userAgent Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Die Benutzer-Agent-Zeichenfolge des Browsers.	userAgent = '*MSIE*'

userAttr.*<auth-attr>* Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter **Wichtig:** Nur die für Rollenzuordnungsregeln ausgewerteten Attribute sind in den detaillierten Rollen (Bedingungen) in den Ressourcenrichtlinien verfügbar.	Von einem LDAP- oder RADIUS-Authentifizierungsserver oder -Verzeichnisserver abgerufene Benutzerattribute.	userAttr.building = ('HQ*' or 'MtView[1-3]') userAttr.dept = ('sales' and 'eng') userAttr.dept = ('eng' or 'it' or 'custsupport') userAttr.division = 'sales' userAttr.employeeType != 'contractor' userAttr.salaryGrade > 10 userAttr.salesConfirmed >= userAttr.salesQuota ***Negative Beispiele:*** userAttr.company != "Acme Inc" or not group.contractors not (user = 'guest' or group.demo) ***Beispiele für Kombinationen:*** *Erlaubt leitenden Angestellten und deren Assistenten den Zugriff von Montag bis Freitag:* userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri) *Erlaubt alle Partner mit dem Status „Aktiv" von Montag bis Freitag, jedoch bevorzugte Partner von Montag bis Samstag:* ((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active'

userDN Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln	Der Benutzer-DN von einem LDAP-Server. Wenn der Benutzer durch den LDAP-Server authentifiziert wird, stammt dieser DN vom Authentifizierungsserver, andernfalls stammt der DN vom Verzeichnis-/Attributserver des Bereichs. Platzhalter sind nicht zulässig.	userDN = 'cn=John Harding,ou=eng,c=Company' userDN = certDN
userDN.*<user-attr>* Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Beliebige Variable aus dem Benutzer-DN, wobei *user-attr* der Name des RDN-Schlüssels ist.	userDN.ou = 'eng'
userDNText Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinien-regeln • Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Benutzer-DN. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	userDNText = 'cn=John Harding,ou=eng,c=Company'

Anhang E.
Benutzerdefinierte Anmeldeseiten

Mit der Funktion der benutzerdefinierten Anmeldeseiten können Sie das Erscheinungsbild der Seiten für Authentifizierungs-Vorabprüfungen und Kennwortverwaltung personalisieren, die das IVE für Administratoren und Endbenutzer bereitstellt. Sie können diese Funktion verwenden, um die in den folgenden Dateien enthaltenen Seiten anzupassen:

- **Sample.zip**

  Diese ZIP-Datei enthält einige IVE-Standardseiten, darunter IVE-Standardseiten, ACE-Seiten und mit Netegrity SiteMinder zu verwendende ACE-Seiten, die sämtlich für Authentifizierungs-Vorabprüfungen verwendet werden, sowie Seiten zur Kennwortverwaltung. Eine vollständige Liste finden Sie unter „Verwenden von Vorlagen aus „samples.zip"" auf Seite 619.

- **SoftID.zip**

  Diese ZIP-Datei enthält mehrere Seiten, die mit dem RSA Soft ID-Client verwendet werden. Eine vollständige Liste finden Sie unter „Verwenden von Vorlagen aus „SoftID.zip"" auf Seite 637.

- **Kiosk.zip**

  Diese ZIP-Datei enthält mehrere Seiten, die von Kiosk-Benutzern verwendet werden. Eine vollständige Liste finden Sie unter „Verwenden von Vorlagen aus „Kiosk.zip"" auf Seite 638.

Zum Anpassen von IVE-Seiten müssen Sie die Template Toolkit-Sprache verwenden. Weitere Informationen finden Sie unter „Informationen zur Template Toolkit-Sprache" auf Seite 614.

Informationen zur Template Toolkit-Sprache

Dieser Abschnitt enthält eine Kurzbeschreibung der Template Toolkit-Sprache für IVE-Benutzer. Es werden die gängigsten Direktiven und Operatoren beschrieben, die von Designern zum Erstellen einer angepassten Seite für das IVE verwendet werden können. Vollständige Informationen zum Template Toolkit finden Sie unter http://www.template-toolkit.org.

Eine mit dem Template Toolkit erstellte Webseite ähnelt einer Standard-webseite. Sie kann HTML, XML und JavaScript enthalten. Im Gegensatz zu einer Standardwebseite kann sie allerdings auch Template Toolkit-Direktiven enthalten, die zum Hinzufügen dynamischen Verhaltens zu Ihren Seiten verwendet werden können.

Eine ***Direktive*** ist eine einfache Anweisung, die die Vorlagenverarbeitung anweist, eine Aktion durchzuführen und die ursprüngliche Direktive im Dokument durch das Ergebnis zu ersetzen. Sie können Direktiven für viele Zwecke verwenden, z. B. zum Durchlaufen einer Liste mit Werten (`FOREACH`), Erstellen von Bedingungsanweisungen (`IF/UNLESS/ELSE`) oder zum Einbeziehen und Verarbeiten einer weiteren Vorlagendatei (`INCLUDE`).

Beachten Sie beim Verwenden von Direktiven im Code Folgendes:

- Bei Direktiven wird die Groß- und Kleinschreibung berücksichtigt, und sie werden IMMER GROSS GESCHRIEBEN.
- Direktiven müssen innerhalb der Markup-Tags **'<%'** und **'%>'** eingefügt werden.

Wichtig: Die Template Toolkit-Dokumentation enthält Beispiele zur Verwendung von Tags mit spitzen und eckigen Klammern, um Direktiven zu markieren. Das IVE unterstützt nur Markup-Tags mit spitzen Klammern.

- Sie können Direktiven an beliebigen Stellen in einer Textzeile einbetten.
- Direktiven können auf mehrere Zeilen verteilt werden.
- Sie können das Zeichen # verwenden, um innerhalb einer Direktive Kommentare einzufügen. Die Template Toolkit-Sprache ignoriert alle Zeichen, die auf das Zeichen # folgen.
- In der Regel ignoriert die Template Toolkit-Sprache überflüssige Leerzeichen innerhalb der Direktive.

Neben der Verwendung von Direktiven ermöglicht die Template Toolkit-Sprache außerdem das Einfügen von Schleifen, Bedingungen, Variablenersetzungen und anderen Vorlagendateien in Ihrer Seite.

In den folgenden Abschnitten werden gängige Template Toolkit-Aufgaben, -Direktiven und -Operationen beschrieben, die Sie in Ihren angepassten Seiten verwenden können:

Informationen über zusätzliche Direktiven wie INCLUDE und INSERT, die Sie innerhalb der Template Toolkit-Sprache verwenden können, finden Sie in der Template Toolkit-Dokumentation, die unter http://www.template-toolkit.org verfügbar ist.

Zugreifen auf und Aktualisieren von Variablen und Dateien

GET-Direktive

Die GET-Direktive ruft den Wert der benannten Variable ab und gibt ihn aus.

```
<% GET foo %>
```

Das Schlüsselwort GET ist optional. Eine Variable kann in einem Direktiventag für sich selbst stehen.

```
<% foo %>
```

SET-Direktive

Mit der SET-Direktive können Sie vorhandenen Variablen einen Wert zuweisen oder neue temporäre Variablen erstellen.

```
<% SET title = 'Hello World' %>
```

Das Schlüsselwort SET ist optional.

```
<% title = 'Hello World' %>
```

Erstellen von Bedingungsanweisungen

Bedingungsoperatoren

Die folgenden Bedingungsoperatoren können verwendet werden:

Operator	Beschreibung
==	gleich
!=	ungleich
<	kleiner als
<=	kleiner oder gleich
>	größer als
>=	größer oder gleich
&&	und
||	oder
!	nicht
and	und
or	oder
not	nicht

IF- und ELSIF-Direktiven

Die IF- und ELSIF-Direktiven können zum Konstruieren bedingten Verhaltens verwendet werden. Beachten Sie, dass es sich dabei um Blockdirektiven handelt. Das bedeutet, dass Sie die END-Direktive zum Angeben des jeweiligen Blockendes verwenden müssen. Sie können Blöcke unbegrenzt schachteln, sofern Sie für jeden geschachtelten Block eine End-Anweisung verwenden.

```
<% IF LoginPageErrorCode == 1002 %>

<b> Your username or password is incorrect. Please reenter your
credentials. </b>

<%ELSIF LoginPageErrorCode == 1006 %>

<b> The system is undergoing maintenance. Only administrators are
allowed to sign in at this time.</b>

<% END %>
```

SWITCH- und CASE-Direktiven

Die SWITCH- und CASE- Direktiven können zum Erstellen eines mehrfachen Bedingungstests verwendet werden. Beachten Sie, dass es sich dabei um Blockdirektiven handelt. Das bedeutet, dass Sie die END-Direktive zum Angeben des jeweiligen Blockendes verwenden müssen. Sie können Blöcke unbegrenzt schachteln, sofern Sie für jeden geschachtelten Block eine End-Anweisung verwenden.

```
<% SWITCH loginPageErrorCode %>

<% CASE 1.001 %>

<b> Your session time has expired. </b>

<% CASE 1006 %>

<b> The system is undergoing maintenance. Only administrators are
permitted to sign in at this time. </b>

<% CASE %> # default ...

<% END %>
```

Erstellen von Schleifenkonstrukten

Direktiven wie FOREACH und WHILE können verwendet werden, um Schleifen in Codeblöcken auszuführen. Beachten Sie, dass es sich dabei um Blockdirektiven handelt. Das bedeutet, dass Sie die END-Direktive zum Angeben des jeweiligen Blockendes verwenden müssen. Sie können Blöcke unbegrenzt schachteln, sofern Sie für jeden geschachtelten Block eine End-Anweisung verwenden.

Der folgende Anmeldeseitencode führt beispielsweise eine Schleife in allen Authentifizierungsbereichen aus und zeigt diese in einer Auswahlliste an. Im Beispiel werden auch die vordefinierten IVE-Werte RealmList und realm verwendet.

```
<select size="1" name="realm">

<% FOREACH r = RealmList %>

<option value="<% r %>"><% r %> </option>

<% END %>

</select>
```

Nicht unterstützte Direktiven

Die USE-, INTERPOLATE-, TAGS-, PERL- und RAWPERL-Direktiven werden von Juniper Networks beim Erstellen von benutzerdefinierten IVE Seiten nicht unterstützt. Außerdem wird die Verwendung der CALL- und FILTER-Direktiven nicht empfohlen.

Verwenden von Vorlagen aus „samples.zip“

Die Datei **samples.zip** enthält die folgenden Vorlagen, die Sie zur Verwendung in Ihrer eigenen Umgebung anpassen können. Beachten Sie, dass alle mit einem Sternchen (*) markierten Vorlagen in der hochgeladenen ZIP-Datei erforderlich sind.

Hinweis: Sie können alle hier aufgeführten Seiten für Pocket PC anpassen. Die Pocket PC-Vorlagen sind mit den anderen in dieser ZIP-Datei enthaltenen Vorlagen identisch, mit der Ausnahme, dass sie für einen kleineren Anzeigebereich angepasst sind und Sie keine dieser Vorlagen zur ZIP-Datei hinzufügen müssen. Alle Pocket PC-Vorlagen verwenden dieselben Namen wie die entsprechenden Vorlagen für die Vollbildanzeige, allerdings wird zu ihren Dateinamen „ppc“ hinzugefügt. Die Anmeldeseitenvorlage für die Vollbildanzeige hat beispielsweise den Namen `LoginPage.thtml`, wohingegen die entsprechende Pocket PC-Datei `LoginPage-ppc.thtml` heißt. Informationen zu Pocket PC-Vorlagen finden Sie im Abschnitt über die entsprechenden Vollbildvorlagen.

IVE-Seiten für Authentifizierungs-Vorabprüfungen

Sie können eine Reihe von IVE-Standardseiten für Authentifizierungs-Vorabprüfungen anpassen, darunter die Standardanmeldeseite (`LoginPage.thtml`), die Seite für fehlgeschlagene Authentifizierung (`SSL.thtml`), die Abmeldeseite (`Logout.thtml`), die Anmeldewarnseite (`ExceededConcurrent.thtml`), die Startseite für die Hostprüfung und die Cachebereinigung (`PleaseWait.thtml`) und die Seite zum Auswählen aus mehreren Rollen (`SelectRole.thtml`).

Hinweis: Alle mit einem Sternchen (*) markierten Vorlagen sind in der hochgeladenen ZIP-Datei erforderlich.

LoginPage.thtml*

Sie müssen immer `LoginPage.thtml` in die ZIP-Datei einschließen, auch dann, wenn Sie einen Authentifizierungsserver verwenden, für den kein Benutzername und kein Kennwort erforderlich sind. Hierbei handelt es sich um die IVE-Standardanmeldeseite, auf der Benutzername, Kennwort und Authentifizierungsbereich des Benutzers erfasst werden und ein Fehler angezeigt wird, wenn die Authentifizierung fehlschlägt. Im Folgenden wird aufgeführt, wo Sie Informationen zum Ausblenden dieser Seite für Benutzer erhalten, die von den jeweiligen Servern authentifiziert werden:

- Anonymer Server: Informationen unter „AnonymousAuthentication“ auf Seite 630
- Zertifikatserver: Informationen unter „CertificateAuthentication“ auf Seite 631
- Netegrity SiteMinder-Server mit clientseitiger Zertifikatauthentifizierung: Informationen unter „Funktion „Login()““ auf Seite 621

JavaScript

Der Header in `LoginPage.thtml` enthält mehrere JavaScript-Funktionen. Die meisten dieser Funktionen sind für die Behandlung von Situationen vorgesehen, in denen mehrere Authentifizierungsbereiche mit einem einzelnen Anmelde-URL verknüpft werden.

Funktion „SetLastRealm(sValue)“

Mit dieser Funktion können Sie es den Benutzern ermöglichen, auf der Anmeldeseite aus mehreren Bereichen auszuwählen. Beim Anmelden des Benutzers ruft diese Funktion den vom Benutzer ausgewählten Authentifizierungsbereich ab und legt ein Ablaufdatum (30 Tage) für die Speicherung durch das IVE fest.

```
function SetLastRealm(sValue) {

var dtExpire = new Date();

dtExpire.setDate(dtExpire.getDate() + 30);

document.cookie = "lastRealm=" +

escape(sValue) + "; expires=" + dtExpire.toGMTString();

}
```

Funktion „Login()“

Diese Funktion umfasst zwei Aktionen:

- **Speicherung des ausgewählten Authentifizierungsbereichs**

  Mit dieser Aktion innerhalb der Funktion können Sie es den Benutzern ermöglichen, auf der Anmeldeseite aus mehreren Bereichen auszuwählen. Die Funktion prüft, ob ein Bereich vorhanden ist, und speichert dann den momentan ausgewählten Authentifizierungsbereich.

- **Festlegen der Zeitzone des Benutzers**

  Erforderlich. Die Funktion verwendet die Variable `tz_offset` (Zeitzonenoffset) und die Funktion `getTimezoneOffset()`, um die Zeitzone des Benutzers zu bestimmen.

```
function Login() {

// Speichern des derzeit ausgewählten Authentifizierungsbereichs

if (document.frmLogin.realm != null &&

document.frmLogin.realm.type == "select-one") {

SetLastRealm(
```

```
 document.frmLogin.realm.options
 [document.frmLogin.realm.selectedIndex].text);

}

if (document.frmLogin.tz_offset != null) {

var wdate = new Date (95, 12, 1);

var sdate = new Date (95, 6, 1);

var winter = (-1) * wdate.getTimezoneOffset();

var summer = (-1) * sdate.getTimezoneOffset();

document.frmLogin.tz_offset.value = winter < summer ? winter :
summer;

}

return true;

}
```

Funktion „GetCookieValue(sName)“

Mit dieser Funktion können Sie es den Benutzern ermöglichen, auf der Anmeldeseite aus mehreren Bereichen auszuwählen. Dies ist eine allgemeine Hilfsfunktion, die einen Wert aus einem Cookie abruft, eine Zeichenfolge von der Länge des Wertes erstellt und die Zeichenfolge dann mit dem Wert füllt.

```
function GetCookieValue(sName) {

var s = document.cookie;

sName += "=";

// Start nv-Paar

var nStart = s.indexOf(sName);
```

```
if (nStart == -1)

return "";

else

nStart += sName.length;

// bei weiteren Werten kürzen, andernfalls den Rest der Zeichenfolge
abrufen

var nEnd = document.cookie.indexOf(";", nStart);

if (nEnd == -1)

s = unescape(s.substring(nStart));

else

s = unescape(s.substring(nStart, nEnd));

return s;

}
```

Funktion „recallLastRealmUsed()“

Mit dieser Funktion können Sie es den Benutzern ermöglichen, auf der Anmeldeseite aus mehreren Bereichen auszuwählen. Die Funktion prüft, ob ein Bereich vorhanden ist, und ruft dann den zuletzt ausgewählten Authentifizierungsbereich ab.

```
function recallLastRealmUsed() {

if (document.frmLogin.realm != null &&

document.frmLogin.realm.type == "select-one") {

// Versuch, den zuletzt verwendeten Authentifizierungsbereich
abzurufen

var sLastRealm = GetCookieValue("lastRealm");
```

```
if (sLastRealm.length > 0) {

var cmb = document.frmLogin.realm;

var nNumRealms = cmb.options.length;

for (var n=0; n < nNumRealms; n++) {

if (cmb.options[n].text == sLastRealm) {

 cmb.selectedIndex = n;

}

}

}

}

}
```

Funktion „FinishLoad()“

Mit dieser Funktion können Sie es den Benutzern ermöglichen, auf der Anmeldeseite aus mehreren Bereichen auszuwählen. Die Funktion prüft, ob ein Bereich vorhanden ist, füllt das Bereichsfeld aus und legt dann den Fokus auf das Benutzernamenfeld. Rufen Sie diese Funktion nach dem vollständigen Laden der Seite auf, um sicherzustellen, dass die erforderlichen Felder vorhanden sind, bevor sie den Fokus erhalten.

```
function FinishLoad() {

recallLastRealmUsed();

if (document.frmLogin.username != null) {

document.frmLogin.username.focus();

}

}
```

Wenn Sie Benutzer über einen Netegrity SiteMinder-Server mit clientseitiger Zertifikatauthentifizierung authentifizieren, möchten Sie möglicherweise die IVE-Standardauthentifizierungsseite für die Benutzer ausblenden. Zum Bereitstellen von Daten für das IVE, ohne die Benutzer zum Eingeben von Anmeldeinformationen aufzufordern, können Sie die folgende geänderte Version der Funktion `FinishLoad()` verwenden. Beachten Sie, dass diese Funktion die Anmeldeseite nur dann umgeht, wenn beim Laden der Seite keine Fehler auftreten:

```
function FinishLoad() {

recallLastRealmUsed();

<% IF !LoginPageErrorCode %>

Login();

document.frmLogin.submit();

<% END %>

}
```

Wenn Sie die Benutzer über einen anonymen Authentifizierungsserver oder Zertifikatauthentifizierungsserver authentifizieren und die IVE-Standard-anmeldeseite umgehen möchten, finden Sie Informationen dazu unter „AnonymousAuthentication“ auf Seite 630 oder „CertificateAuthentication“ auf Seite 631.

Formularfelder

`LoginPage.thtml` enthält mehrere Formularfelder, die Sie bereitstellen müssen:

tz_offset

Erforderlich. Die Funktion `Login()` verwendet den Wert von `tz_offset` (Zeitzonenoffset), um die Zeitzone des Benutzers zu bestimmen.

```
<input type="hidden" name="tz_offset">
```

username

Dieses Feld ist für alle Typen von Authentifizierungsservern erforderlich, mit Ausnahme von anonymen Servern und Zertifikatservern. `Login.cgi` (ein Perl-Skript auf dem IVE) gibt den hier bereitgestellten Wert für den `Benutzernamen` an den entsprechenden Authentifizierungsserver weiter.

```
<input type="text" name="username">
```

password

Dieses Feld ist für alle Typen von Authentifizierungsservern erforderlich, mit Ausnahme von anonymen Servern und Zertifikatservern. `Login.cgi` gibt den hier bereitgestellten Wert für das `Kennwort` an den entsprechenden Authentifizierungsserver weiter.

```
<input type="password" name="password">
```

realm

Erforderlich. `Login.cgi` gibt den hier bereitgestellten Wert für den `Bereich` an den entsprechenden Authentifizierungsserver weiter.

```
<% IF RealmList.size == 0 %>

<td>LoginRealm</td><td> </td><td>

<input type="text" name="realm" size="20">

</td>

<% ELSIF RealmList.size == 1 %>

<input type="hidden" name="realm" value="<% RealmList.0 %>"">

<% ELSE %>

<td>LoginRealm</td><td> </td><td>

<select size="1" name="realm">

<% FOREACH r = RealmList %>
```

```
<option value="<% r %>" ><% r %></option>

<% END %>

</select>
```

Formulardefinition

`LoginPage.thtml` enthält die folgende vorgeschlagene Formulardefinition. Innerhalb dieser Formulardefinition sind die meisten Elemente erforderlich:

```
<form name="frmLogin" action="login.cgi" method="post"
autocomplete="off" onsubmit="return Login()">
```

name

(Erforderlich) Legt den Formularnamen fest. Dieser Name wird von IVE Servercode verwendet.

```
name="frmLogin"
```

action

(Erforderlich) Führt das Perl-Skript `login.cgi` auf dem IVE aus.

```
action="login.cgi"
```

method

(Erforderlich) Stellt den Wert im Formular für `login.cgi` bereit.

```
method="post"
```

autocomplete

(Optional) Verhindert, dass das Formular automatisch mithilfe von zwischengespeicherten Werten mit Feldeinträgen für Benutzername oder Authentifizierungsbereich ausgefüllt wird.

```
autocomplete="off"
```

onsubmit

(Erforderlich bei Verwendung von Secure Meeting) Gibt den von der Funktion `Login()` festgelegten Wert für das Zeitzonenoffset zurück.

```
onsubmit="return Login()"
```

Variablen

In dieser Vorlage können Sie folgende Variablen verwenden:

LoginPageErrorMessage

Erforderlich. IVE-Fehlermeldungstext, den Sie Benutzern anzeigen können. Dieser Text entspricht einem von `LoginPageErrorCode` zurückgegebenen Code. Beachten Sie, dass Sie diesen Text auf dem IVE nicht ändern können. Sie können aber Code in Ihre Vorlage einfügen, um anderen Text anzuzeigen, der auf dem von der Variable `LoginPageErrorCode` zurückgegebenen Fehlercode basiert. Beispiel:

```
<% IF LoginPageErrorCode == 1002 %>

<b> Your username or password is incorrect. Please reenter your
credentials. </b>

<%ELSIF LoginPageErrorCode == 1006 %>

<b> The system is undergoing maintenance. Only administrators are
allowed to sign in at this time.</b>

<% END %>
```

LoginPageErrorCode

Codes für die Fehler, die Sie Benutzern anzeigen können. Im Folgenden werden Fehler, die Benutzern auf dieser Seite möglicherweise angezeigt werden, und der von der Variable `LoginPageErrorMessage` zurückgegebene entsprechende Text erläutert:

Fehlermeldung	Fehlercode	Kommentare
Invalid Username or Password	1002	
This login requires a digital certificate.	1003	
The digital certificate is invalid.	1004	
Only admins are permitted to login.	1006	
Logins are not permitted using this browser	1008	
There are no auth servers defined for this user.	1009	
Exceeded the number of concurrent users.	1010	
The IP has been blocked due too many concurrent sign-in attempts.	1011	
The password is too short.	1012	
Sign on for administrators is disabled. You can try again in a few minutes.	1018	Dies wird angezeigt, wenn ein Superadministrator angemeldet ist und sich das IVE im Wiederherstellungsmodus befindet.
Your New PIN has been saved. Please make sure to remember it.	1019	Verwendung nur bei ACE-Authentifizierung.
Password Change Success	1020	Verwendung mit der Kennwortverwaltungsfunktion.
Account Disabled	1021	Verwendung mit der Kennwortverwaltungsfunktion.
Account Locked out	1022	Verwendung mit der Kennwortverwaltungsfunktion.
Account Expired	1023	Verwendung mit der Kennwortverwaltungsfunktion.
This realm has reached the max session limit.	1027	

Fehlermeldung	Fehlercode	Kommentare
Access denied. Please try signing in again using a hostname (for example, https://department.yourcompany) instead of an IP address (such as http://10.11.12.13)	1029	Verwendung nur bei Netegrity SiteMinder-Authentifizierung.
You do not have the correct privileges to access the system. Please contact your administrator for more information.	1030	

RealmList

Liste mit für Benutzer verfügbaren Bereichen.

Home

Verweist auf das Verzeichnis der obersten Ebene in Ihrer ZIP-Datei. Zum Verweisen auf das Verzeichnis der obersten Ebene können Sie diese Variable oder die Konvention „..“ verwenden. Im folgenden Beispiel sind beide Verweise gültig:

```
<% Home %>/images/logo.gif
```

```
../images/logo.gif
```

AnonymousAuthentication

Das IVE legt diesen Wert auf „true“ fest, wenn der Authentifizierungsbereich auf einen anonymen Server festgelegt ist. Sie können diese Variable verwenden, um festzulegen, dass für Benutzer, die sich an einem anonymen Bereich anmelden, auf der Anmeldeseite die Felder für Benutzername und Kennwort nicht angezeigt werden. In diesem Fall zeigt das IVE den Benutzern die Anmeldeseite nur dann an, wenn einer der unter „LoginPageErrorCode“ auf Seite 629 beschriebenen Fehler auftritt.

CertificateAuthentication

Das IVE legt diesen Wert auf „true“ fest, wenn der Authentifizierungsbereich auf einen Zertifikatserver festgelegt ist. Sie können diese Variable verwenden, um festzulegen, dass für Benutzer, die sich an einem Zertifikatbereich anmelden, auf der Anmeldeseite die Felder für Benutzername und Kennwort nicht angezeigt werden. In diesem Fall zeigt das IVE den Benutzern die Anmeldeseite nur dann an, wenn einer der unter „LoginPageErrorCode“ auf Seite 629 beschriebenen Fehler auftritt. (Informationen zum Ausblenden dieser Seite für Benutzer, die über einen Netegrity SiteMinder-Server mit clientseitiger Zertifikatauthentifizierung authentifiziert werden, finden Sie unter „Funktion „Login()““ auf Seite 621.)

Logout.thtml*

`Logout.thtml` muss immer in Ihre ZIP-Datei eingebunden werden. Dabei handelt es sich um eine IVE-Standardseite, auf der ein Fehler angezeigt wird, wenn sich ein Benutzer abmeldet, wenn eine Zeitüberschreitung bei der Benutzersitzung auftritt oder wenn das IVE die Hostprüfung oder die Cachebereinigung vom System des Benutzers deinstalliert.

Diese Vorlage enthält JavaScript zum Erkennen, Beenden, Installieren und Deinstallieren der Komponenten Hostprüfung und Cachebereinigung, Bilder und Text, die Benutzern angezeigt werden, während das IVE diese Aktionen durchführt, und JavaScript zum Schließen und Öffnen des J-SAM-Fensters.

Diese Vorlage enthält auch Variablen, die die Benutzer während der Installation von Komponenten zum Warten auffordern, eine Verknüpfung, mit der sich Benutzer erneut am IVE anmelden können, sowie Variablen für Fehlermeldungen.

Beachten Sie beim Konfigurieren der in dieser Vorlage enthaltenen Variable `LoginPageErrorMessage`, dass der vom IVE für Benutzer angezeigte Text Code entspricht, der von `LoginPageErrorCode` zurückgegeben wurde. Diesen Text können Sie auf dem IVE nicht ändern. Sie können aber Code in Ihre Vorlage einfügen, um anderen Text anzuzeigen, der auf dem von der Variable `LoginPageErrorCode` zurückgegebenen Fehlercode basiert. Beispiel:

```
<% IF LoginPageErrorCode == 1001 %>

<b> Your secure gateway session has ended due to inactivity.</b>

<% END %>
```

Im Folgenden werden die möglichen Fehler aufgeführt, die `LoginPageErrorCode` zurückgeben kann, sowie der von der Variable `LoginPageErrorMessage` zurückgegebene entsprechende Text:

Fehlermeldung	Fehlercode
Maximum Session Timeout Reached.	1000
Idle Time Out.	1001

Detaillierte Informationen über das hier aufgeführte JavaScript und die beschriebenen Variablen finden Sie in den Kommentaren in der Vorlage.

ExceededConcurrent.thtml*

`ExceededConcurrent.thtml` muss immer in Ihre ZIP-Datei eingebunden werden. Hierbei handelt es sich um eine IVE-Standardseite, die dem Benutzer eine Leistungswarnung anzeigt, wenn zu viele Benutzer gleichzeitig am IVE angemeldet sind. Diese Vorlage enthält kein JavaScript und keine Formulare. Sie enthält allerdings eine optionale Verknüpfung mit `starter.cgi`, über die sich Benutzer beim IVE anmelden können, sowie Fehlermeldungsvariablen. Weitere Informationen finden Sie in den Kommentaren in der Vorlage.

SSL.thtml*

`SSL.thtml` muss immer in Ihre ZIP-Datei eingebunden werden. Hierbei handelt es sich um eine IVE-Standardseite, auf der bei fehlgeschlagener Authentifizierung eine Fehlermeldung angezeigt wird, woraufhin sich der Benutzer nicht mehr beim IVE anmelden kann. Diese Vorlage enthält kein JavaScript und keine Formulare. Sie enthält allerdings Fehlermeldungsvariablen. Weitere Informationen finden Sie in den Kommentaren in der Vorlage.

PleaseWait.thtml

Sie können diese Vorlage anpassen, wenn Sie die Hostprüfung oder die Cachebereinigung auf Bereichsebene konfiguriert haben. Verwenden Sie diese Seite, um das Starten der Hostprüfung und der Cachebereinigung vor und nach der Authentifizierung zu steuern.

Diese Vorlage enthält JavaScript zum Erkennen, Beenden, Installieren und Deinstallieren der Komponenten Hostprüfung und Cachebereinigung sowie Bilder und Text, die Benutzern angezeigt werden, während das IVE diese Aktionen durchführt. Sie enthält außerdem JavaScript zum regelmäßigen Überprüfen des Benutzerstatus. Dadurch wird bestimmt, ob die Hostprüfung oder die Cachebereinigung auf dem System des Benutzers geladen ist, und der Benutzer wird ggf. auf die Anmeldeseite (`welcome.cgi`) umgeleitet.

Diese Vorlage enthält außerdem Variablen, die die Benutzer zum Warten während der Installation von Komponenten auffordern, eine Fehlermeldungsvariable, eine Variable zum Speichern der Uhrzeit, zu der die Seite zum ersten Mal geladen wird, und eine Statusvariable für die Komponenten Hostprüfung und Cachebereinigung.

Detaillierte Informationen über das hier aufgeführte JavaScript und die beschriebenen Variablen finden Sie in den Kommentaren in der Vorlage.

SelectRole.thtml

Wenn Sie die Benutzer zu mehreren Rollen zugewiesen, aber diese Rollen nicht permissiv zusammengeführt haben, können Sie diese Vorlage anpassen. Diese Seite wird nach der Anmeldeseite eingeblendet und zeigt eine Liste mit Rollen an, aus der der Benutzer auswählen kann. Detaillierte Informationen zum optionalen JavaScript, zur Formulardefinition, zu den Formularfeldern und Variablen dieser Vorlage finden Sie in den Kommentaren in der Vorlage.

ACE-Seiten für Authentifizierungs-Vorabprüfungen

Sie können fünf ACE-Seiten für Authentifizierungs-Vorabprüfungen anpassen:

- **NewPin.thtml**

  Diese Vorlage fordert ACE-Benutzer auf, eine neue PIN einzugeben oder vor der Anmeldung beim IVE eine vom System erzeugte PIN zu erstellen. Beachten Sie beim Konfigurieren der Variable `secid_pinselectmode` (die den PIN-Auswahlmodus des Benutzers festlegt), dass folgende Werte möglich sind:

Modus	Beschreibung
0	Der Benutzer muss die vom System erstellte PIN verwenden. Es kann keine eigene PIN eingegeben werden.
1	Der Benutzer kann seine eigene PIN eingeben oder die vom System erstellte PIN verwenden.
2	Der Benutzer muss seine eigene PIN eingeben. Die vom System erstellte PIN kann nicht verwendet werden.

  Beachten Sie, dass beim Konfigurieren der Variable `secid_pinserr` (die den Fehlercode und die Meldung über die falsche Eingabe der PIN speichert) folgende Werte möglich sind:

Code	Wert
0	Neue PIN erforderlich.
1	Die beiden eingegebenen PINs stimmen nicht überein.
2	Ungültiges PIN-Format.
3	Ungültige PIN-Länge.

- **NextToken.thtml**

  Diese Vorlage fordert den Benutzer auf, durch Eingeben seines SecurID-Tokencodes seine Anmeldeinformationen zu überprüfen.

- **GeneratePin.thtml**

  Diese Vorlage ermöglicht dem Benutzer das Erstellen einer von System erzeugten ID. Beachten Sie beim Konfigurieren der Variable `secid_pinselectmode` (die den PIN-Auswahlmodus des Benutzers festlegt), dass folgende Werte möglich sind:

Modus	Beschreibung
0	Der Benutzer muss die vom System erstellte PIN verwenden. Es kann keine eigene PIN eingegeben werden.
1	Der Benutzer kann seine eigene PIN eingeben oder die vom System erstellte PIN verwenden.
2	Der Benutzer muss seine eigene PIN eingeben. Die vom System erstellte PIN kann nicht verwendet werden.

- **ShowSystemPin.thtml**

  Diese Vorlage zeigt dem Benutzer die vom System erzeugte PIN an.

- **Cancel.thtml**

  Diese Vorlage zeigt dem Benutzer eine Informationsmeldung darüber an, dass seine Anmeldeanforderung abgebrochen wurde.

Informationen über das JavaScript sowie die Formulardefinitionen, Formularfelder und Variablen in diesen Vorlagen finden Sie in den Kommentaren der Vorlagen.

ACE-Seiten mit Netegrity für Authentifizierungs-Vorabprüfungen

Sie können vier ACE-Seiten für Authentifizierungs-Vorabprüfungen anpassen, die mit Netegrity SiteMinder verwendet werden:

- **SM-NewPinSelect.thtml**

  Diese Vorlage fordert den Benutzer auf, eine neue PIN einzugeben oder vor der Anmeldung beim IVE eine vom System erzeugte PIN zu erstellen.

- **SM-NewPinSystem.thtml**

  Mit dieser Vorlage können Benutzer eine vom System erzeugte PIN erstellen, wenn auf der Seite `SM-NewPinSelect.thtml` die Option für eine System-PIN ausgewählt wurde.

- **SM-NewUserPin.thtml**

  Diese Vorlage fordert den Benutzer auf, eine neue PIN zu erstellen, wenn auf der Seite `SM-NewPinSelect.thtml` die Option zum Eingeben einer PIN ausgewählt wurde. Sie bestimmt außerdem, ob die vom Benutzer eingegebenen beiden PINs übereinstimmen, und benachrichtigt

gegebenenfalls den Benutzer. Beachten Sie, dass beim Konfigurieren der Variable `secid_pinserr` (die den Fehlercode und die Meldung über die falsche Eingabe der PIN speichert) folgende Werte möglich sind:

Code	Wert
0	Zuweisung einer neuen PIN
1	Die beiden eingegebenen PINs stimmen nicht überein

- **SM-NextToken.thtml**

  Diese Vorlage fordert den Benutzer auf, durch Eingeben seines SecurID-Tokencodes seine Anmeldeinformationen zu überprüfen.

Informationen über das JavaScript sowie die Formulardefinitionen, Formularfelder und Variablen in diesen Vorlagen finden Sie in den Kommentaren der Vorlagen.

Seiten zur Kennwortverwaltung

Sie können vier Seiten zur Kennwortverwaltung anpassen:

- **Defender.thtml**

  Diese Vorlage fordert den Radius-Benutzer auf, seine PIN einzugeben, und stellt die entsprechenden Anfragewerte vom Server bereit.

- **GraceLoginUsed.thtml**

  Diese Vorlage informiert den Benutzer darüber, wie oft er sich noch mit seinem aktuellen Benutzernamen und Kennwort anmelden kann.

- **PasswordChange.thtml**

  Diese Vorlage benachrichtigt den Benutzer, dass sein Kennwort bald abläuft, und fordert ihn auf, es zu ändern.

- **PasswordExpiration.thtml**

  Diese Vorlage benachrichtigt den Benutzer, dass sein Kennwort abgelaufen ist, und fordert ihn auf, es zu ändern.

Informationen über das JavaScript sowie die Formulardefinitionen, Formularfelder und Variablen in diesen Vorlagen finden Sie in den Kommentaren der Vorlagen.

Verwenden von Vorlagen aus „SoftID.zip“

Mit der Datei **SoftID.zip** können Sie IVE-Seiten zur Verwendung mit dem RSA Soft ID-Client anpassen. Diese ZIP-Datei enthält folgende Vorlagen:

- **Cancel.thtml**

  Diese Vorlage ermöglicht dem Benutzer das Erstellen einer von System erzeugten ID. Weitere Informationen finden Sie unter „Cancel.thtml“ auf Seite 635.

- **ExceededConcurrent.thtml**

  Diese Vorlage zeigt dem Benutzer eine Leistungswarnung an, wenn zu viele Benutzer gleichzeitig beim IVE angemeldet sind. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

- **LoginPage.thtml**

  Diese Vorlage ruft den RSA Soft ID-Client auf und ermöglicht es dem Benutzer, sich beim IVE mit Soft ID-Authentifizierung anzumelden. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

- **Logout.thtml**

  Diese Vorlage zeigt einen Fehler an, wenn sich ein Benutzer abmeldet, wenn eine Zeitüberschreitung bei der Benutzersitzung auftritt oder wenn das IVE die Hostprüfung oder die Cachebereinigung vom System des Benutzers deinstalliert. Detailliertere Informationen finden Sie unter „Logout.thtml*“ auf Seite 631. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

- **NewPin.thtml**

  Diese Vorlage fordert ACE-Benutzer auf, eine neue PIN einzugeben oder vor der Anmeldung beim IVE eine vom System erzeugte PIN zu erstellen. Weitere Informationen finden Sie unter „NewPin.thtml“ auf Seite 634.

- **NextToken.thtml**

  Diese Vorlage fordert den Benutzer auf, durch Eingeben seines SecurID-Tokencodes seine Anmeldeinformationen zu überprüfen.

- **PleaseWait.thtml**

  Diese Vorlage erkennt, beendet, installiert und deinstalliert die Komponenten Hostprüfung oder Cachebereinigung, zeigt Benutzern Bilder und Text an, während das IVE diese Aktionen durchführt, prüft regelmäßig den Status des Benutzers, um zu bestimmen, ob die Hostprüfung oder die Cachebereinigung auf seinem System geladen ist, und leitet ihn gegebenenfalls auf die Anmeldeseite (`welcome.cgi`) um. Weitere Informationen finden Sie unter „PleaseWait.thtml“ auf Seite 633.

- **SelectRole.thtml**

  Diese Vorlagenseite wird nach der Anmeldeseite eingeblendet und zeigt eine Liste mit Rollen an, aus der der Benutzer auswählen kann. Wenn Sie die Benutzer zu mehreren Rollen zugewiesen, aber diese Rollen nicht permissiv zusammengeführt haben, können Sie diese Vorlage anpassen.

- **SSL.thtml**

  Diese Vorlage zeigt einen Fehler an, wenn die Authentifizierung fehlschlägt und der Benutzer sich nicht beim IVE anmelden kann. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

Hinweis: Sie können alle hier aufgeführten Seiten für Pocket PC anpassen. Die Pocket PC-Vorlagen sind mit den anderen in dieser ZIP-Datei enthaltenen Vorlagen identisch, mit der Ausnahme, dass sie für einen kleineren Anzeigebereich angepasst sind und Sie keine dieser Vorlagen zur ZIP-Datei hinzufügen müssen. Alle Pocket PC-Vorlagen verwenden dieselben Namen wie die entsprechenden Vorlagen für die Vollbildanzeige, allerdings wird zu ihren Dateinamen „ppc“ hinzugefügt. Die Anmeldeseitenvorlage für die Vollbildanzeige hat beispielsweise den Namen `LoginPage.thtml`, wohingegen die entsprechende Pocket PC-Datei `LoginPage-ppc.thtml` heißt. Informationen zu Pocket PC-Vorlagen finden Sie im Abschnitt über die entsprechenden Vollbildvorlagen.

Verwenden von Vorlagen aus „Kiosk.zip“

Mit der Datei **Kiosk.zip** können Sie IVE-Seiten zur Verwendung für Kiosk-Benutzer anpassen. Diese ZIP-Datei enthält folgende Vorlagen:

- **Cancel.thtml**

  Diese Vorlage ermöglicht dem Benutzer das Erstellen einer von System erzeugten ID. Weitere Informationen finden Sie unter „Cancel.thtml“ auf Seite 635.

- **ExceededConcurrent.thtml**

  Diese Vorlage zeigt dem Benutzer eine Leistungswarnung an, wenn zu viele Benutzer gleichzeitig beim IVE angemeldet sind. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

- **GeneratePin.thtml**

  Diese Vorlage ermöglicht dem Benutzer das Erstellen einer von System erzeugten ID. Weitere Informationen finden Sie unter „GeneratePin.thtml“ auf Seite 635.

- **keyboarddemo.thtml**

  Diese Vorlage enthält HTML-Beispiele, mit denen Benutzer aufgefordert werden, Daten ohne Verwendung der Tastatur einzugeben. Die Eingabe ohne Tastatur hilft dabei, Angriffe durch Tastaturprotokollierung zu verhindern.

- **LoginPage.thtml**

  Diese Vorlage ermöglicht es den Benutzern, sich mit Soft ID-Authentifizierung beim IVE anzumelden. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

- **Logout.thtml**

  Diese Vorlage zeigt einen Fehler an, wenn sich ein Benutzer abmeldet, wenn eine Zeitüberschreitung bei der Benutzersitzung auftritt oder wenn das IVE die Hostprüfung oder die Cachebereinigung vom System des Benutzers deinstalliert. Detailliertere Informationen finden Sie unter „Logout.thtml*“ auf Seite 631. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

- **NewPin.thtml**

  Diese Vorlage fordert ACE-Benutzer auf, eine neue PIN einzugeben oder vor der Anmeldung beim IVE eine vom System erzeugte PIN zu erstellen. Weitere Informationen finden Sie unter „NewPin.thtml“ auf Seite 634.

- **NextToken.thtml**

  Diese Vorlage fordert den Benutzer auf, durch Eingeben seines SecurID-Tokencodes seine Anmeldeinformationen zu überprüfen.

- **PleaseWait.thtml**

  Diese Vorlage erkennt, beendet, installiert und deinstalliert die Komponenten Hostprüfung und Cachebereinigung, zeigt Benutzern Bilder und Text an, während das IVE diese Aktionen durchführt, prüft regelmäßig den Status des Benutzers, um zu bestimmen, ob die Hostprüfung und Cachebereinigung auf seinem System geladen ist, und leitet ihn gegebenenfalls auf die Anmeldeseite (`welcome.cgi`) um. Weitere Informationen finden Sie unter „PleaseWait.thtml“ auf Seite 633.

- **ShowSystemPin.thtml**

  Diese Vorlage zeigt dem Benutzer die vom System erzeugte PIN an.

- **SSL.thtml**

  Diese Vorlage zeigt einen Fehler an, wenn die Authentifizierung fehlschlägt und der Benutzer sich nicht beim IVE anmelden kann. Diese Vorlage muss immer in Ihre ZIP-Datei eingebunden werden.

Hinweis: Sie können alle hier aufgeführten Seiten für Pocket PC anpassen. Die Pocket PC-Vorlagen sind mit den anderen in dieser ZIP-Datei enthaltenen Vorlagen identisch, mit der Ausnahme, dass sie für einen kleineren Anzeigebereich angepasst sind und Sie keine dieser Vorlagen zur ZIP-Datei hinzufügen müssen. Alle Pocket PC-Vorlagen verwenden dieselben Namen wie die entsprechenden Vorlagen für die Vollbildanzeige, allerdings wird zu ihren Dateinamen „ppc“ hinzugefügt. Die Anmeldeseitenvorlage für die Vollbildanzeige hat beispielsweise den Namen `LoginPage.thtml`, wohingegen die entsprechende Pocket PC-Datei `LoginPage-ppc.thtml` heißt. Informationen zu Pocket PC-Vorlagen finden Sie im Abschnitt über die entsprechenden Vollbildvorlagen.

Anhang F.
Verwenden des W-SAM-Startprogramms

Das W-SAM-Startprogramm dient zur Anmeldung eines Benutzers am IVE und zum anschließenden Herunterladen und Starten von W-SAM. Für das Startprogramm ist keine Benutzeraktion erforderlich. Stattdessen wird eine Befehlszeilenschnittstelle bereitgestellt, die von einem Skript oder einer Anwendung aufgerufen werden kann. Sie können z. B. eine Anwendung schreiben, die die ausführbare Datei von W-SAM bei Bedarf aufruft.

Für die Anwendung des W-SAM-Startprogramms müssen Sie die folgenden beiden Vorgänge durchführen:

- Schreiben Sie ein Skript, eine Batchdatei oder eine Anwendung, die das W-SAM-Startprogramm über Befehlszeilenargumente aufruft. Verteilen Sie diese Datei an alle Client-PCs, für die dies erforderlich ist.
- Laden Sie das W-SAM-Startprogramm vom IVE herunter, und verteilen Sie es an die Benutzer.

Verwenden Sie die Befehlszeilenargumente in Tabelle 4, um das W-SAM-Startprogramm aufzurufen.

Tabelle 4: W-SAM Befehlszeilenargumente

Argument	Aktion
-start	Initiiert die W-SAM-Verbindung.
-stop	Beendet die W-SAM-Verbindung und meldet den Benutzer ab.
-version	Zeigt die aktuellen W-SAM-Versionsinformationen an und wird dann beendet.
-help	Zeigt verfügbare Argumente an.
-noupgrade	Deaktiviert die automatische Aktualisierung der W-SAM-Software.

Tabelle 4: W-SAM Befehlszeilenargumente fortgesetzt

Argument	Aktion
-reboot	Startet nach Aufforderung durch eine Aktualisierung automatisch neu. Wenn das Flag zum Neustart nicht gesetzt ist, wird W-SAM beendet und startet während einer Aktualisierung nicht neu. Wenn W-SAM auf einem Remote-PC automatisch ausgeführt wird, sollten Sie auf jeden Fall das Flag zum Neustart setzen.
-u <Benutzer>	Gibt den Benutzernamen an.
-p <Kennwort>	Gibt das Kennwort für die Authentifizierung an.
-loginscript file	Gibt den Dateinamen und Speicherort der Skriptdatei an, die beim Starten von W-SAM ausgeführt werden soll. Dieser Befehl hat Vorrang vor einer auf der Seite **Users > Roles >** *Rollenname* **> SAM > Options** angegebenen Skriptdatei.
-postscript file	Gibt den Dateinamen und Speicherort der Skriptdatei an, die beim Beenden von W-SAM ausgeführt werden soll. Dieser Befehl hat Vorrang vor einer auf der Seite **Users > Roles >** *Rollenname* **> SAM > Options** angegebenen Skriptdatei.
-u <URL>	Gibt den Anmelde-URL für das IVE an.
-r <Bereich>	Gibt den Bereich an, an den das IVE die Anmeldeinformationen des Benutzers sendet.
-verbose	Fordert Benutzer über Dialogfelder zu Eingaben auf.

In Tabelle 5 werden die möglichen Codes aufgeführt, die das W-SAM-Startprogramm beim Beenden übergibt.

Tabelle 5: Anwendungsrückgabecodes

Code	Beschreibung
0	Erfolg
1	Ungültige Argumente
2	Es konnte keine Verbindung hergestellt werden
3	Ungültige Anmeldeinformationen
4	Rolle nicht angegeben (Anmeldeinformationen können mehreren Rollen zugeordnet werden)
5	Fehler vor der Authentifizierung (Hostprüfung oder Cachebereinigung wurde nicht geladen)
6	Installation fehlgeschlagen
7	Neustart erforderlich (wenn „reboot" nicht angegeben wurde)

Manuelles Ausführen von Skripts

Die Benutzer können bei Beginn oder Ende einer W-SAM-Sitzung die auszuführenden Skripts manuell mit Befehlszeilenargumenten angeben. Wenn Sie auf der Seite **Users > Roles >** *Rollenname* **> SAM > Options** Skript angegeben haben, die über die Webkonsole ausgeführt werden sollen, wird das konfigurierte Skript nicht ausgeführt, wenn ein Benutzer W-SAM manuell über das Startprogramm aufruft und ein anderes Skript angibt.

So starten Sie ein Skript nach Beginn einer W-SAM Sitzung:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-loginscript file
```

und unmittelbar dahinter eine Systemvariable oder den Dateinamen und Speicherort einer Skriptdatei.

So starten Sie ein Skript nach dem Ende einer W-SAM-Sitzung:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-postscript file
```

und unmittelbar dahinter eine Systemvariable oder den Dateinamen und Speicherort einer Skriptdatei.

Hinweis:

- Setzen Sie Systemvariablen, Dateipfade und Dateinamen in Anführungszeichen.
- Setzen Sie vor und nach Systemvariablen ein Prozentzeichen (%).

Beispiel:

```
-loginscript file "%program files:%\Internet Explorer\IEXPLORER.EXE"
```

Automatisches Ausführen von Skripts

Beispielbatchdatei

Im folgenden Beispiel wird gezeigt, wie Sie W-SAM über das W-SAM-Startprogramm aufrufen. Die Beispielbatchdatei erzeugt beim Start von W-SAM Fehlermeldungen:

```
SamControl -start -url %1 -user %2 -password %3 -realm %4
if errorlevel 1 goto error_invalid_args
if errorlevel 2 goto error_connect
if errorlevel 3 goto error_credentials
if errorlevel 4 goto error_role
if errorlevel 5 goto error_preauth
if errorlevel 6 goto error_install
if errorlevel 7 goto error_reboot


:error_invalid_args
@echo invalid arguments
goto done

:error_connect
@echo could not connect
goto done

:error_credentials
@echo invalid credentials
goto done

:error_role
@echo invalid role
goto done

:error_preauth
@echo pre auth version checking
goto done

:error_install
@echo install failed
goto done

:error_reboot
@echo reboot required
goto done
```

```
:error_success
@echo Secure Application Manager has started
goto done

:done
```

Win32 API-Beispiel

```
CHAR szCmd = “SamLauncher.exe –stop”;
DWORD dwExitCode = 0;
STARTUPINFO si;
PROCESS_INFORMATION pi;
ZeroMemory(&si, sizeof(si));
si.cb = sizeof(si);
ZeroMemory(&pi, sizeof(pi));
if (!CreateProcess(NULL, szCmd, NULL, NULL, FALSE,
    0, NULL, NULL, &si, &pi)) {
    printf( "CreateProcess(%s) failed %d", szCmd, GetLastError());
    return -1;
}
WaitForSingleObject(pi.hProcess, 20000);
GetExitCodeProcess(&pi.hProcess, &dwExitCode);
CloseHandle(pi.hProcess);
CloseHandle(pi.hThread);
printf(“SamLauncher return %d\n”, dwExitCode);
return 0;
```

Index

B

E

F

J

K

L

M

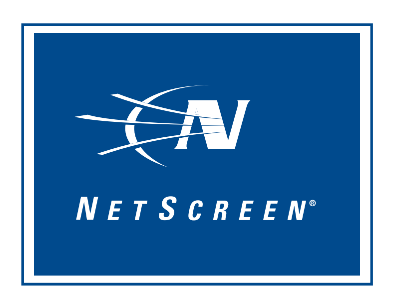
Q

R

S

T

U


NETSCREEN®